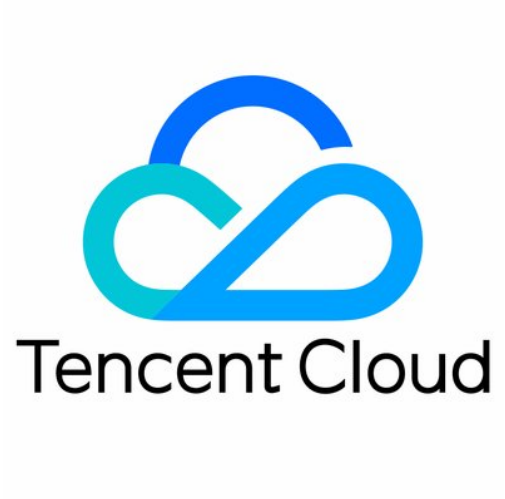
# Cloud Virtual Machine

# Panduan Operasi

## Dokumen produk



# Direktori dokumen

# Panduan Operasi

# Ikhtisar Panduan Operasi

Waktu update terbaru：2021-12-13 17:07:02

Dokumen ini memberikan ikhtisar tentang instans CVM dan kasus penggunaannya. Dokumen ini juga menjelaskan cara mengoperasikan instans CVM.

## Membeli dan Menggunakan CVM

Jika ini pertama kalinya Anda membeli dan menggunakan instans CVM, sebaiknya ikuti petunjuk di bawah ini untuk memulai.

1. Untuk mempelajari tentang instans CVM: lihat Ringkasan CVM.
2. Pilih dan beli model CVM yang sesuai. Jika ini pertama kalinya Anda menggunakan instans CVM sebagai pengguna pribadi, lihat Menyesuaikan Konfigurasi CVM Linux.
3. Login ke instans CVM yang Anda beli: Bergantung pada jenis instans yang dibeli, Anda dapat memilih untuk login ke instans Windows atau instans Linux.

## Menyesuaikan Konfigurasi CVM

Anda mungkin perlu menyesuaikan jenis disk, jaringan, atau konfigurasi lain dari instans CVM karena tuntutan yang berubah. Lihat dokumen berikut untuk membuat perubahan yang sesuai.

Mengubah Konfigurasi Instans

Menyesuaikan Konfigurasi Jaringan

Menyesuaikan Konfigurasi Proyek

Menginstal Ulang Sistem

## Mengatur Ulang Kata Sandi dan Kunci

Jika Anda lupa kata sandi atau kunci Anda hilang, lihat dokumen berikut untuk mengatur ulang kata sandi atau kunci:

Mengatur Ulang Kata Sandi Instans

Mengelola Kunci SSH

## Memperbarui Instans dan Penagihan

Lihat Memperbarui Instans.

# Membuat, Mengimpor, atau Menghapus Citra Kustom

Citra memberikan informasi yang diperlukan untuk meluncurkan instans CVM. Tencent Cloud menyediakan empat jenis citra: citra publik, citra marketplace, citra kustom, dan citra bersama. Saat ini kami mendukung operasi terkait citra berikut.

Membuat Citra Kustom

Menghapus Citra Kustom

Mengimpor Citra

Menyalin Citra

### Pemecahan Masalah

Saat Anda tidak dapat login ke instans CVM, atau jika Anda mengalami respons lambat atau masalah lain, lihat hal berikut untuk pemecahan masalah:

Kegagalan Login CVM

Latensi Jaringan CVM dan Kehilangan Paket

# Ikhtisar Batas Penggunaan

Waktu update terbaru：2024-05-16 11:02:11

## Batas Akun untuk Membeli Instans CVM

Anda harus mendaftar untuk akun Tencent Cloud. Untuk informasi selengkapnya, lihat Mendaftar untuk Akun Tencent Cloud.
Jika Anda membuat CVM bayar sesuai pemakaian, sistem akan menangguhkan biaya penggunaan CVM selama satu jam. Pastikan bahwa akun Anda memiliki saldo yang cukup untuk melakukan pemesanan.

## Batas Penggunaan Instans CVM

Perangkat lunak virtual tidak dapat diinstal atau divirtualisasi ulang (seperti menginstal VMware atau Hyper-V).
Anda tidak dapat menggunakan kartu suara atau memasang perangkat keras eksternal (seperti flash drive USB, disk eksternal, dan tombol U).
CVM gateway publik hanya tersedia di sistem operasi Linux.

## Batas Pembelian Instans CVM

Untuk setiap pengguna, **quota** (kuota) instans CVM bayar sesuai pemakaian di setiap zona ketersediaan adalah 30.
Untuk informasi selengkapnya, lihat Batas Pembelian.

## Batas Citra

Citra publik: tidak ada batasan penggunaan.
Citra kustom: setiap wilayah mendukung maksimal 10 citra kustom.
Citra yang dibagikan: setiap citra kustom dapat dibagikan kepada maksimal 500 pengguna Tencent Cloud. Citra kustom hanya dapat dibagikan dengan akun di wilayah yang sama dengan akun sumber.
Untuk informasi selengkapnya, lihat Jenis Citra.

## Batas EIP

**Batas Kuota**

| Sumber Daya | Batas |
| --- | --- |
| Jumlah EIP untuk setiap akun Tencent Cloud di setiap wilayah | 20 |
| Jumlah aplikasi pembelian harian untuk setiap akun Tencent Cloud di setiap wilayah | Kuota * 2 |
| Frekuensi alamat IP publik dapat dipindahkan ke setiap akun secara gratis per hari saat EIP tidak terikat | 10 |

**Batasan pada IP publik yang terikat ke CVM**

Mulai tanggal 18 September 2019, jumlah maksimum IP publik yang dapat diikat ke satu CVM telah diubah berdasarkan konfigurasi CPU. Kuota ditampilkan seperti di bawah ini:

**Keterangan:**

Batasan ini tidak berlaku untuk instans CVM yang dibeli sebelum pukul 00.00, 18 September 2019. Untuk instans ini, jumlah IP publik yang dapat diikat ke setiap instans sama dengan jumlah IP pribadi yang didukung oleh server Anda.

| Jumlah CPU pada CVM | Jumlah maksimum IP publik yang dapat diikat (termasuk IP publik dan elastis) |
| --- | --- |
| 1-5 | 2 |
| 6-11 | 3 |
| 12-17 | 4 |
| 18-23 | 5 |
| 24-29 | 6 |
| 30-35 | 7 |
| 36-41 | 8 |
| 42-47 | 9 |
| ≥ 48 | 10 |

# Batas ENI

Berdasarkan konfigurasi CPU dan memori, jumlah ENI yang terikat ke CVM berbeda dengan jumlah IP pribadi yang terikat ke ENI. Kuota tersebut seperti yang ditunjukkan di bawah ini:

**Perhatian:**

Jumlah alamat IP yang terikat pada satu ENI menunjukkan jumlah maksimum yang diizinkan. Kuota EIP tidak diberikan berdasarkan batas atas ini tetapi berdasarkan EIP batas penggunaan.

Number of ENIs bound to a CVM instance

Number of private IPs bound to a single ENI on CVM instances

| Model | Jenis Instans | Jumlah ENI | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | CPU: 1 core | CPU: 2 core | CPU: 4 core | CPU: 6 core | CPU: 8 core | CPU: 10 core | CPU: 12 core | CPU: 14 core | |
| Standar | S5 Standar | 2 | 4 | 4 | - | 6 | - | - | - | |
| | S5se yang Dioptimalkan Penyimpanan Standar | - | - | 4 | - | 6 | - | - | - | |
| | SA2 Standar | 2 | 4 | 4 | - | 6 | - | - | - | |
| | S4 Standar | 2 | 4 | 4 | - | 6 | - | - | - | |
| | SN3ne yang Dioptimalkan Jaringan Standar | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| | S3 Standar | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| | SA1 Standar | 2 | 2 | 4 | - | 6 | - | - | - | |
| | S2 Standar | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| | S1 Standar | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| IO tinggi | IO IT5 tinggi | - | - | - | - | - | - | - | - | |
| | IO IT3 tinggi | - | - | - | - | - | - | - | - | |
| MEM Dioptimalkan | M5 yang Dioptimalkan Memori | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| | M4 yang Dioptimalkan Memori | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| | M3 yang | 2 | 4 | 4 | - | 6 | - | 8 | - | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Dioptimalkan Memori | | | | | | | | | |
| | M2 yang Dioptimalkan Memori | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| | M1 yang Dioptimalkan Memori | 2 | 4 | 4 | - | 6 | - | 8 | - | |
| Komputasi | C4 yang Dioptimalkan Komputasi | - | - | 4 | - | 6 | - | - | - | |
| | CN3 yang dioptimalkan untuk Jaringan Komputasi | - | - | 4 | - | 6 | - | - | - | |
| | Komputasi C3 | - | - | 4 | - | 6 | - | - | - | |
| | Komputasi C2 | - | - | 4 | - | 6 | - | - | - | |
| Berbasis GPU | Komputasi GPU GN6 | - | - | - | - | - | - | - | - | |
| | Komputasi GPU GN6S | - | - | 4 | - | 6 | - | - | - | |
| | Komputasi GPU GN7 | - | - | 4 | - | 6 | - | - | - | |
| | Komputasi GPU GN8 | - | - | - | 4 | - | - | - | 8 | |
| | Komputasi GPU GN10X | - | - | - | - | 6 | - | - | - | |
| | Komputasi GPU GN10Xp | - | - | - | - | - | 6 | - | - | |
| Big Data | Big Data D3 | - | - | - | - | 6 | - | - | - | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Big Data D2 | - | - | - | - | 6 | - | - | - | |

| Model | Jenis Instans | Jumlah IP pribadi yang terikat pada satu ENI | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | CPU: 1 core | CPU: 2 core | CPU: 4 core | CPU: 6 core | CPU: 8 core | CPU: 10 core | CPU: 12 core | CPU: 14 core |
| Standar | S5 Standar | 6 | 10 | 10 | - | 20 | - | - | - |
| | S5se yang Dioptimalkan Penyimpanan Standar | - | - | 20 | - | 20 | - | - | - |
| | SA2 Standar | 6 | 10 | 10 | - | 20 | - | - | - |
| | S4 Standar | 6 | 10 | 10 | - | 20 | - | - | - |
| | SN3ne yang Dioptimalkan Jaringan Standar | 6 | 10 | 10 | - | 20 | - | 30 | - |
| | S3 Standar | 6 | 10 | 10 | - | 20 | - | 30 | - |
| | SA1 Standar | Memori 1 GB: Memori 2>1 GB: 6 | 10 | Memori 8 GB: Memori 1016 GB: 20 | - | 20 | - | - | - |
| | S2 Standar | 6 | 10 | 10 | - | 20 | - | 30 | - |
| | S1 Standar | 6 | 10 | 10 | - | 20 | - | 30 | - |
| IO tinggi | IO IT5 tinggi | - | - | - | - | - | - | - | - |
| | IO IT3 tinggi | - | - | - | - | - | - | - | - |
| MEM Dioptimalkan | M5 yang Dioptimalkan Memori | 6 | 10 | 10 | - | 20 | - | 30 | - |
| | M4 yang Dioptimalkan | 6 | 10 | 10 | - | 20 | - | 30 | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Memori | | | | | | | | |
| | M3 yang Dioptimalkan Memori | 6 | 10 | 10 | - | 20 | - | 30 | - |
| | M2 yang Dioptimalkan Memori | 6 | 10 | 10 | - | 20 | - | 30 | - |
| | M1 yang Dioptimalkan Memori | 6 | 10 | 10 | - | 20 | - | 30 | - |
| Komputasi | C4 yang Dioptimalkan Komputasi | - | - | 10 | - | 20 | - | - | - |
| | CN3 yang dioptimalkan untuk Jaringan Komputasi | - | - | 10 | - | 20 | - | - | - |
| | Komputasi C3 | - | - | 10 | - | 20 | - | - | - |
| | Komputasi C2 | - | - | 10 | - | 20 | - | - | - |
| Berbasis GPU | Komputasi GPU GN2 | - | - | - | - | - | - | - | - |
| | Komputasi GPU GN6 | - | - | - | - | - | - | - | - |
| | Komputasi GPU GN6S | - | - | 10 | - | 20 | - | - | - |
| | Komputasi GPU GN7 | - | - | 10 | - | 20 | - | - | - |
| | Komputasi GPU GN8 | - | - | - | 10 | - | - | - | 30 |
| | Komputasi GPU GN10X | - | - | - | - | 20 | - | - | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Komputasi GPU GN10Xp | - | - | - | - | - | 20 | - | - |
| Berbasis FPGA | FPGA Accelerated FX4 | - | - | - | - | - | 20 | - | - |
| Big Data | Big Data D3 | - | - | - | - | 20 | - | - | - |
| | Big Data D2 | - | - | - | - | 20 | - | - | - |
| | Big Data D1 | - | - | - | - | 20 | - | - | - |
| Mesin Fisik Cloud 2.0 | | Tidak didukung | | | | | | | |

# Batas Bandwidth

Bandwidth keluar maksimum (bandwidth hilir)

Aturan berikut berlaku untuk instans yang dibuat sebelum pukul 00:00, 24 Februari 2020:

| Metode Penagihan Jaringan | Instans | | Rentang Bandwidth Maksimum (Mbps) |
|---|---|---|---|
| | Metode Penagihan Instans | Konfigurasi Instans | |
| Tagihan per lalu lintas | Instans berbasis pembayaran sesuai pemakaian | Semua | 0-100 |
| Tagihan per bandwidth | Instans berbasis pembayaran sesuai pemakaian | Semua | 0-100 |
| Paket Bandwidth | Semua | | 0-2000 |

Aturan berikut berlaku untuk instans yang dibuat setelah pukul 00.00, 24 Februari 2020:

| Metode Penagihan Jaringan | Instans | | Rentang Bandwidth Maksimum (Mbps) |
|---|---|---|---|
| | Metode Penagihan Instans | Konfigurasi Instans | |
| Tagihan per lalu lintas | Instans berbasis pembayaran sesuai pemakaian | Semua | 0-100 |

| | | | |
|---|---|---|---|
| Tagihan per bandwidth | Instans berbasis pembayaran sesuai pemakaian | Semua | 0-100 |
| Paket Bandwidth | Semua | | 0-2000 |

Bandwidth masuk maksimum (bandwidth hulu)
Jika bandwidth tetap yang Anda beli lebih besar dari 10 Mbps, Tencent Cloud akan menetapkan bandwidth masuk jaringan publik sama dengan bandwidth yang dibeli.
Jika bandwidth tetap yang Anda beli kurang dari 10 Mbps, Tencent Cloud akan menetapkan bandwidth masuk jaringan publik 10-Mbps.

## Batas Disk

| Batasan | Deskripsi |
|---|---|
| Kemampuan disk cloud elastis | Mulai dari Mei 2018, semua disk data yang dibeli dengan CVM adalah disk cloud elastis, yang dapat dilepas dari dan dipasang kembali ke CVM. Fitur ini didukung di semua zona ketersediaan. |
| Performa disk cloud elastis | Spesifikasi I/O berlaku untuk performa input dan output secara bersamaan.Misalnya, jika SSD 1 TB memiliki IOPS acak maksimum 26.000, artinya performa baca dan tulisnya dapat mencapai nilai ini. Karena batasan performa, jika ukuran blok dalam contoh ini adalah 4 KB atau 8 KB, IOPS maksimum dapat dicapai. Jika ukuran blok 16 KB, IOPS maksimum tidak dapat dicapai (throughput telah mencapai batas 260 MB/dtk.) |
| Jumlah disk cloud elastis yang dipasang ke CVM | Maksimum 20 |
| Jumlah snapshot dalam satu wilayah | 64 + Jumlah disk cloud di wilayah tersebut x 64 |
| Disk cloud yang dipasang ke CVM | CVM dan disk cloud harus berada di zona ketersediaan yang sama. |
| Pengembalian snapshot | Data snapshot hanya dapat dikembalikan ke disk cloud tempat snapshot dibuat. |

| | |
|---|---|
| Jenis disk cloud dapat dibuat menggunakan snapshot | Hanya snapshot dari disk data yang dapat digunakan untuk membuat disk cloud elastis baru. |
| Ukuran disk cloud yang dibuat menggunakan snapshot | Ukuran disk cloud yang dibuat menggunakan snapshot harus lebih besar atau sama dengan disk cloud sumber. |

# Batas Grup Keamanan

Grup keamanan bersifat khusus wilayah. CVM hanya dapat diikat ke grup keamanan di wilayah yang sama.
Grup keamanan berlaku untuk instans CVM di lingkungan jaringan mana pun.
Setiap pengguna dapat mengonfigurasi maksimum 50 grup keamanan untuk setiap proyek di suatu wilayah.
Maksimal 100 aturan masuk atau keluar dapat dikonfigurasi untuk grup keamanan.
Satu CVM dapat dikaitkan dengan beberapa grup keamanan, dan grup keamanan dapat dikaitkan dengan beberapa instans CVM.
Grup keamanan yang terkait dengan CVM di **classic network** (jaringan klasik) tidak dapat memfilter paket dari atau ke database TencentDB (MySQL, MariaDB, SQL Server, atau PostgreSQL) dan NoSQL (Redis atau Memcached). Sebagai gantinya, Anda dapat menggunakan iptables untuk memfilter lalu lintas untuk instans tersebut.
Kuota tersebut ditunjukkan seperti di bawah ini:

| Item | Batas |
|---|---|
| Jumlah grup keamanan | 50 per wilayah |
| Jumlah aturan dalam grup keamanan | 100 untuk aturan masuk dan 100 untuk aturan keluar |
| Jumlah instans CVM yang terkait dengan grup keamanan | 2.000 |
| Jumlah grup keamanan yang terkait dengan instans CVM | 5 |
| Jumlah grup keamanan yang dapat dirujuk oleh grup keamanan | 10 |

# Batas VPC

| Sumber Daya | Batas |
| --- | --- |
| Jumlah VPC per wilayah untuk setiap akun | 20 |
| Jumlah subnet per VPC | 100 |
| Jumlah CVM berbasis jaringan klasik dapat dikaitkan dengan setiap instans VPC | 100 |
| Jumlah tabel rute per VPC | 10 |
| Jumlah tabel rute yang terkait dengan setiap subnet | 1 |
| Jumlah kebijakan perutean per tabel rute | 50 |
| Jumlah HAVIP default per VPC | 10 |

# Instans

# Membuat Instans

# Pedoman untuk Membuat Instans

Waktu update terbaru：2021-12-13 17:07:02

Dokumen ini memperkenalkan beberapa metode pembuatan instans CVM, mulai dari operasi dasar hingga fitur kustom lanjutan.

Membuat instans CVM melalui halaman pembelian CVM adalah metode yang paling umum digunakan. Hal ini memungkinkan Anda secara fleksibel memilih konfigurasi yang memenuhi kebutuhan bisnis Anda. Untuk informasi selengkapnya, lihat Membuat Instans melalui Halaman Pembelian CVM.

Jika Anda ingin menggunakan sistem operasi, aplikasi, atau konfigurasi lain yang Anda kenal, Anda dapat membuat citra kustom terlebih dahulu dan memilihnya saat membuat instans untuk meningkatkan efisiensi. Untuk informasi selengkapnya, lihat Membuat Instans melalui Citra.

Jika Anda ingin membeli instans dengan konfigurasi yang sama dengan instans saat ini, Anda dapat langsung membuat instans dengan konfigurasi yang sama. Untuk informasi selengkapnya, lihat Membeli dengan Konfigurasi yang Sama.

# Membuat Instans melalui Halaman Pembelian CVM

Waktu update terbaru：2023-04-21 15:39:59

## Ikhtisar

Dokumen ini memandu Anda melalui cara membuat instans Tencent Cloud Virtual Machine (CVM) menggunakan mode konfigurasi kustom sebagai contoh.

## Prasyarat

Sebelum membuat instans CVM, Anda harus menyelesaikan langkah-langkah berikut:
Daftar untuk akun Tencent Cloud dan selesaikan verifikasi identitas sebelum membeli instans CVM apa pun di daratan China.
Untuk membuat instans CVM yang jenis jaringannya adalah virtual private cloud (VPC), Anda perlu membuat VPC di wilayah target, dan membuat subnet di zona ketersediaan target di bawah VPC.
Jika Anda tidak menggunakan proyek default, Anda perlu membuat proyek.
Jika Anda tidak menggunakan grup keamanan default, Anda perlu buat grup keamanan di wilayah target dan menambahkan aturan grup keamanan yang memenuhi persyaratan bisnis Anda.
Untuk mengikat pasangan kunci SSH saat membuat instans Linux, Anda perlu membuat kunci SSH untuk proyek target.
Untuk membuat instans CVM dengan citra kustom, Anda perlu membuat citra kustom atau mengimpor citra.

## Petunjuk

1. Login ke Tencent Cloud. Pilih **Products** (Produk) -> **Compute and Container** -> **Compute** (Komputasi) -> **Cloud Virtual Machine** ([Cloud Virtual Machine]). Klik **Get Started** (Mulai) untuk mengakses halaman pembelian CVM.
Custom Configuration**:** ([Konfigurasi Kustom]:) Mode ini cocok untuk kasus penggunaan tertentu. Mode ini memungkinkan pengguna membeli instans CVM sesuai kebutuhan khusus mereka.
2. Konfigurasi informasi berikut seperti yang diminta oleh halaman:

| Kategori | Wajib/Opsional | Deskripsi Konfigurasi |
| --- | --- | --- |
| Mode Penagihan | Wajib | Harap pilih berdasarkan kebutuhan aktual Anda:<br>**Bayar sesuai pemakaian**: mode penagihan elastis untuk CVM. |

| | | |
|---|---|---|
| | | Untuk informasi selengkapnya tentang mode penagihan, lihat Mode Penagihan Instans. |
| Wilayah/Zona Ketersediaan | Wajib | **Wilayah**: sebaiknya pilih wilayah terdekat dengan pelanggan Anda guna mengurangi latensi akses dan meningkatkan kecepatan akses.<br>**Zona ketersediaan**: pilih berdasarkan kebutuhan aktual.Jika Anda ingin membeli beberapa CVM, kami sarankan Anda memilih zona ketersediaan yang berbeda untuk diterapkan pemulihan bencana.<br>Untuk informasi selengkapnya tentang wilayah dan zona ketersediaan, lihat<br>Wilayah dan Zona Ketersediaan. |
| Jaringan | Wajib | Ruang jaringan yang terisolasi secara logis yang dibangun di Tencent Cloud. Virtual private cloud (VPC) mencakup setidaknya satu subnet. Sistem ini menyediakan VPC dan subnet default untuk setiap wilayah. Jika VPC atau subnet yang sudah ada tidak memenuhi persyaratan Anda, Anda dapat membuat VPC atau subnet di konsol VPC.<br>**Catatan**:<br>Sumber daya di VPC yang sama dapat dibagikan dalam jaringan pribadi. Saat membeli CVM, pastikan CVM dan subnet tempat CVM dibuat memiliki zona ketersediaan yang sama. |
| Instans | Wajib | Tencent Cloud menyediakan berbagai jenis instans berdasarkan perangkat keras yang mendasarinya. Untuk performa yang optimal, sebaiknya gunakan jenis instans generasi terbaru.<br>Untuk informasi selengkapnya tentang instans, lihat Jenis Instans. |
| Citra | Wajib | Tencent Cloud menyediakan citra publik, citra kustom, dan citra bersama.<br>Untuk informasi selengkapnya tentang citra, lihat Ikhtisar. |
| Disk Sistem | Wajib | Digunakan untuk menginstal sistem operasi. Kapasitas defaultnya adalah 50 GB.Jenis Cloud Block Storage (CBS) yang tersedia berbeda-beda, bergantung pada wilayahnya. Harap pilih nilai seperti yang diinstruksikan oleh halaman.<br>Untuk informasi selengkapnya tentang CBS, lihat Jenis Disk Cloud. |
| Disk Data | Opsional | Digunakan untuk meningkatkan kapasitas penyimpanan CVM guna memastikan efisiensi dan keandalan yang tinggi. Disk data CBS tidak ditambahkan secara default.<br>Untuk mengetahui informasi selengkapnya tentang Jenis Disk Cloud, lihat Jenis CBS. |
| Bandwidth Jaringan Publik | Wajib | Secara default, IP publik khusus akan diberikan secara gratis.<br>Tencent Cloud menyediakan dua mode penagihan jaringan.<br>Konfigurasikan nilai yang lebih besar dari 0 Mbps sesuai kebutuhan.<br>**Tagihan per bandwidth**: pilih bandwidth tetap. Kehilangan paket akan terjadi ketika bandwidth melebihi nilai ini. Ini berlaku untuk skenario ketika |

| | | |
|---|---|---|
| | | koneksi jaringan sedikit berfluktuasi.<br>**Tagihan per lalu lintas**: penagihan didasarkan pada lalu lintas yang benar-benar digunakan. Anda dapat menentukan bandwidth puncak untuk mencegah biaya yang ditimbulkan oleh lalu lintas yang tidak terduga. Kehilangan paket akan terjadi ketika bandwidth instan melebihi nilai ini. Ini berlaku untuk skenario di mana koneksi jaringan berfluktuasi secara signifikan.<br>**Paket tagihan per bandwidth**: pilih penagihan gabungan ini ketika instans jaringan publik Anda memiliki puncak lalu lintas pada waktu yang berbeda. Ini berlaku untuk bisnis skala besar di mana lalu lintas dapat berubah-ubah antara berbagai instans menggunakan jaringan publik.BWP saat ini dalam versi beta. Untuk mencobanya, harap kirimkan aplikasi beta.<br>**Catatan**:<br>IP publik khusus gratis yang ditetapkan tidak dapat dilepaskan dari instans. Untuk melepaskan alamat IP ini, pertama-tama konversikan IP publik ke IP elastis. Untuk informasi selengkapnya tentang IP elastis, lihat IP Elastis (EIP).<br>Alamat IP publik khusus tidak dapat ditetapkan dalam dua kasus berikut. Harap lihat halaman pembelian untuk informasi terbaru.<br>Sumber daya IP telah terjual habis<br>Di wilayah tertentu |
| Gateway Publik | Opsional | Hanya berlaku untuk citra Linux.<br>Sebagai antarmuka jaringan antara VPC dan jaringan publik, gateway publik dapat meneruskan permintaan CVM yang berada dalam subnet VPC yang berbeda dan tidak memiliki alamat IP publik.<br>**Catatan**: Tencent Cloud menghentikan konfigurasi gateway publik di halaman pembelian CVM setelah tanggal 6 Desember 2019. Untuk mengonfigurasi gateway publik, lihat Mengonfigurasi Gateway Publik. |
| Kuantitas | Wajib | Jumlah CVM yang akan dibeli. |

3. Klik **Next (Selanjutnya): Complete Configuration** (Selesaikan Konfigurasi) untuk mengakses halaman konfigurasi CVM.

4. Konfigurasi informasi berikut seperti yang diminta oleh halaman:

| Kategori | Wajib/Opsional | Deskripsi Konfigurasi |
|---|---|---|
| Proyek | Wajib | Proyek default dipilih. Anda dapat memilih proyek yang ada sesuai kebutuhan untuk mengelola CVM yang berbeda. |
| Grup Keamanan | Wajib | Jika tidak ada grup keamanan yang tersedia, Anda dapat memilih Grup keamanan baru. |

| | | |
|---|---|---|
| | | Jika ada grup keamanan yang tersedia, Anda dapat memilih Grup Keamanan yang Ada.<br>Untuk informasi selengkapnya tentang grup keamanan, lihat Grup Keamanan. |
| Nama Instans | Opsional | Anda dapat menyesuaikan nama CVM yang akan dibuat.<br>Jika tidak ada nama instans yang ditentukan, **unnamed** (Belum diberi nama) akan digunakan secara default.<br>Nama instans tidak boleh lebih dari 60 karakter. Penamaan Urutan Batch atau Penamaan Berbasis String Pola juga didukung.<br>**Catatan**: nama ini hanya ditampilkan di konsol. Nama ini bukan nama host dari CVM. |
| Metode Login | Wajib | Konfigurasikan metode untuk login ke CVM sesuai kebutuhan.<br>**Atur Kata Sandi**: sesuaikan kata sandi untuk login ke instans.<br>**Pasangan Kunci SSH (hanya untuk instans Linux)**: kaitkan instans dengan kunci SSH untuk memastikan login yang aman ke CVM.Jika tidak ada kunci yang tersedia atau kunci yang sudah ada tidak sesuai, klik **Buat Sekarang** untuk membuat kunci. Untuk informasi selengkapnya tentang kunci SSH, lihat Kunci SSH.<br>**Kata Sandi Acak**: kata sandi yang dibuat secara otomatis akan dikirim melalui Pusat Pesan. |
| Penguatan Keamanan | Opsional | Secara default, Anti-DDoS dan Perlindungan Beban Kerja Cloud diaktifkan secara gratis untuk membantu Anda membangun sistem keamanan CVM guna mencegah kebocoran data. |
| Platform yang dapat diamati Tencent Cloud | Opsional | Secara default, Platform yang dapat diamati Tencent Cloud diaktifkan secara gratis. Anda dapat menginstal komponen untuk mendapatkan metrik pemantauan CVM dan menampilkannya dalam grafik visual. Anda juga dapat menentukan ambang alarm khusus.<br>Selain itu, Anda dapat mengonfigurasi pemantauan data CVM tiga dimensi, analisis data cerdas, alarm kesalahan waktu nyata, dan laporan data khusus untuk secara tepat memantau kondisi kesehatan layanan Tencent Cloud dan CVM. |
| Pengaturan Lanjutan | Opsional | Konfigurasikan pengaturan tambahan untuk instans sesuai kebutuhan.<br>**Nama host**: Anda dapat menyesuaikan nama komputer dalam sistem operasi CVM. Setelah CVM dibuat, Anda dapat login ke CVM untuk melihat nama host.<br>**Grup Penempatan**: Anda dapat menambahkan instans ke grup penempatan sesuai kebutuhan untuk meningkatkan ketersediaan layanan. Untuk informasi selengkapnya, lihat Grup Penempatan.<br>**Tag**: Anda dapat menetapkan tag untuk mengelola sumber daya CVM berdasarkan kategori. Untuk informasi selengkapnya, lihat Mengelola Instans melalui Tag. |

| | | |
|---|---|---|
| | | **Data Kustom**: Anda dapat mengonfigurasi instans dengan menetapkan data kustom, dan skrip yang dikonfigurasi akan berjalan saat instans diluncurkan. Jika beberapa CVM dibeli bersamaan, data kustom akan berjalan di semua CVM. Sistem operasi Linux mendukung format Shell sedangkan sistem operasi Windows mendukung format PowerShell. Maksimum 16 KB data mentah didukung. Untuk informasi selengkapnya, lihat Mengonfigurasi Data Kustom (Linux CVM).<br>**Catatan**: konfigurasi data kustom hanya mendukung citra umum tertentu dengan layanan Cloud-init. Untuk informasi selengkapnya, lihat Cloud-Init & Cloudbase-Init. |

5. Klik **Next (Selanjutnya): Confirm Configuration** (Konfirmasi Konfigurasi) untuk mengakses halaman konfirmasi informasi konfigurasi.
6. Validasi informasi CVM yang akan dibeli dan detail biaya setiap item konfigurasi.
7. Baca dan pilih **Agree "Tencent Cloud Service Terms"** (Setujui "Persyaratan Layanan Tencent Cloud").
8. Klik **Enable** (Aktifkan) dan selesaikan pembayaran. Kemudian, Anda dapat masuk ke konsol CVM untuk melihat CVM Anda.

Informasi seperti nama instans, alamat IP publik, alamat IP pribadi, nama pengguna login, dan kata sandi login awal CVM akan dikirimkan ke akun Anda melalui Pusat Pesan. Anda dapat menggunakan informasi ini untuk login dan mengelola instans Anda. Untuk memastikan keamanan CVM Anda, ubah kata sandi login CVM Anda sesegera mungkin.

# Menciptakan contoh melalui pencerminan kustom

Waktu update terbaru：2021-12-13 17:07:02

## Ikhtisar

Anda dapat menggunakan cira kustom untuk membuat instans CVM dari sistem operasi, aplikasi, dan data yang sama untuk meningkatkan efisiensi. Dokumen ini memandu Anda melalui cara membuat instans menggunakan citra kustom.

## Prasyarat

Anda harus memiliki citra kustom di bawah akun Anda dan di wilayah tempat Anda ingin membuat instans.
Jika tidak ada citra kustom, lihat solusi berikut:

| Status Citra | Solusi |
| --- | --- |
| Citra di komputer lokal atau platform lain | Impor citra disk sistem di komputer lokal atau platform lain ke citra kustom di CVM. Untuk informasi selengkapnya, lihat Ikhtisar. |
| Ada instans templat tetapi tidak ada citra kustom | Untuk informasi selengkapnya, lihat Membuat Citra Kustom. |
| Citra kustom di wilayah lain | Salin citra kustom ke wilayah target tempat Anda ingin membuat instans. Untuk informasi selengkapnya, lihat Menyalin Citra. |
| Citra kustom di bawah akun lain | Bagikan citra kustom dengan akun tempat Anda ingin membuat instans. Untuk informasi selengkapnya, lihat Membagikan Citra Kustom. |

## Petunjuk

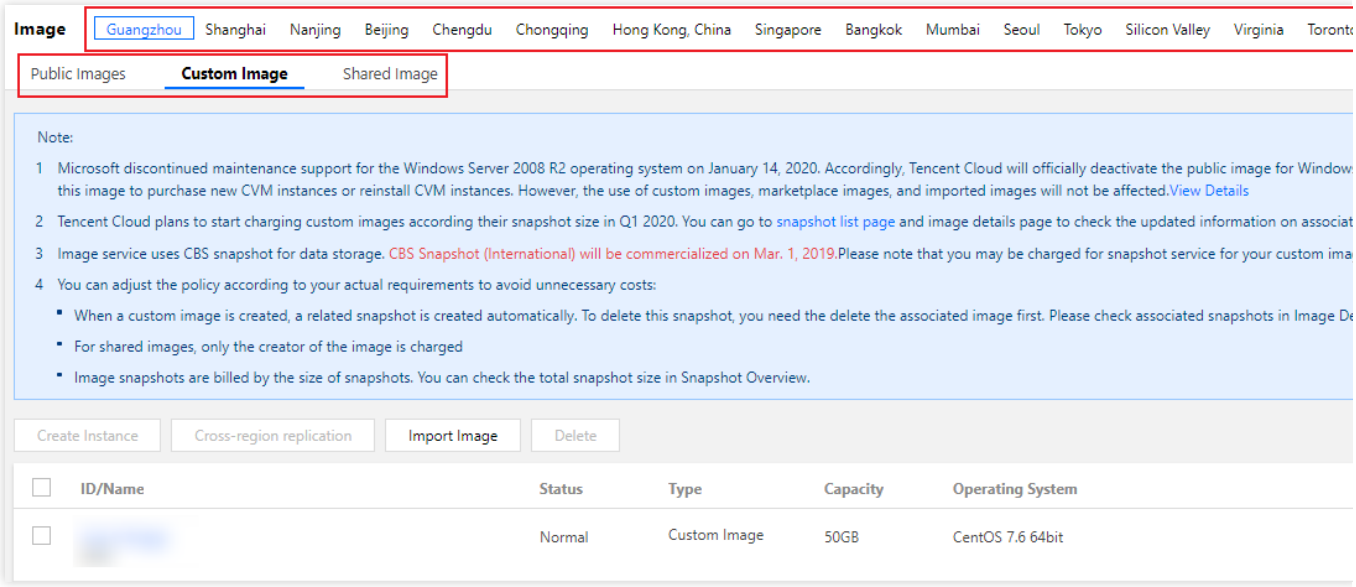
1. Login ke Konsol CVM.
2. Klik **Images** (Citra) di bilah sisi kiri untuk mengakses halaman **Image** (Citra).
3. Pilih wilayah di bagian atas halaman **Image** (Citra).
4. Pilih tab berdasarkan sumber citra untuk melihat daftar citranya.

**Public Image** (Citra Publik): buka halaman citra publik.

**Custom Image** (Citra Kustom): buka halaman citra kustom.

**Shared Image** (Citra Bersama): buka halaman citra bersama.

5. Di bawah kolom **Operation** (Operasi) dari citra yang ingin Anda gunakan, klik **Create Instance** (Buat Instans).




6. Di jendela pop-up, klik **OK** (OKE).

7. Konfigurasikan dan buat instans seperti yang diminta oleh halaman.

Kolom **Region** (Wilayah) dan **Image** (Citra) otomatis akan terisi. Selesaikan konfigurasi instans lainnya sesuai kebutuhan. Untuk informasi selengkapnya, lihat Membuat Instans melalui Halaman Pembelian CVM.

**Keterangan:**

Jika Anda menggunakan citra kustom yang berisi satu atau beberapa snapshot disk data, sistem operasi akan secara otomatis membuat jumlah Cloud Block Storage (CBS) yang sama sebagai snapshot dan kapasitas yang sama dengan setiap snapshot. Anda dapat memperluas, tetapi tidak dapat mengurangi, kapasitas CBS.

# Dokumentasi Terkait

Anda juga dapat membuat citra kustom menggunakan RunInstances API. Untuk informasi selengkapnya, lihat RunInstances.

# Membeli dengan Konfigurasi yang Sama

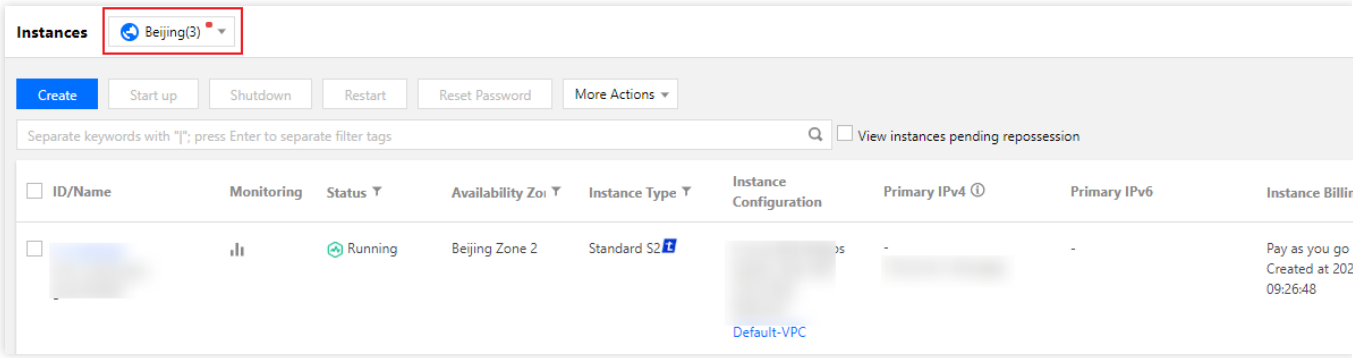
Waktu update terbaru：2021-12-13 17:07:02

## Ikhtisar

Jika Anda ingin membeli lagi instans dengan konfigurasi yang sama, Anda dapat menggunakan fitur **Purchase with same configurations** (Beli dengan konfigurasi yang sama) di Konsol CVM untuk menghemat waktu dan meningkatkan efisiensi penskalaan.

## Petunjuk

1. Login ke Konsol CVM.
2. Pilih wilayah di bagian atas halaman **Instances** (Instans)
3. Di bawah kolom **Operation** (Operasi) pada instans, klik **More** (Lainnya) -> **Purchase with same configurations** (Beli dengan konfigurasi yang sama).




4. Masukkan jumlah CVM yang ingin Anda beli dan periksa konfigurasi lain yang dipilih secara otomatis.
Anda dapat menyesuaikan konfigurasi parameter berdasarkan kebutuhan aktual Anda.
5. Klik **Purchase** (Beli) dan selesaikan pembayaran.

# Membuat Skrip API Explorer yang Dapat Digunakan Kembali untuk Membuat Instans

Waktu update terbaru：2021-12-13 17:07:03

## Ikhtisar

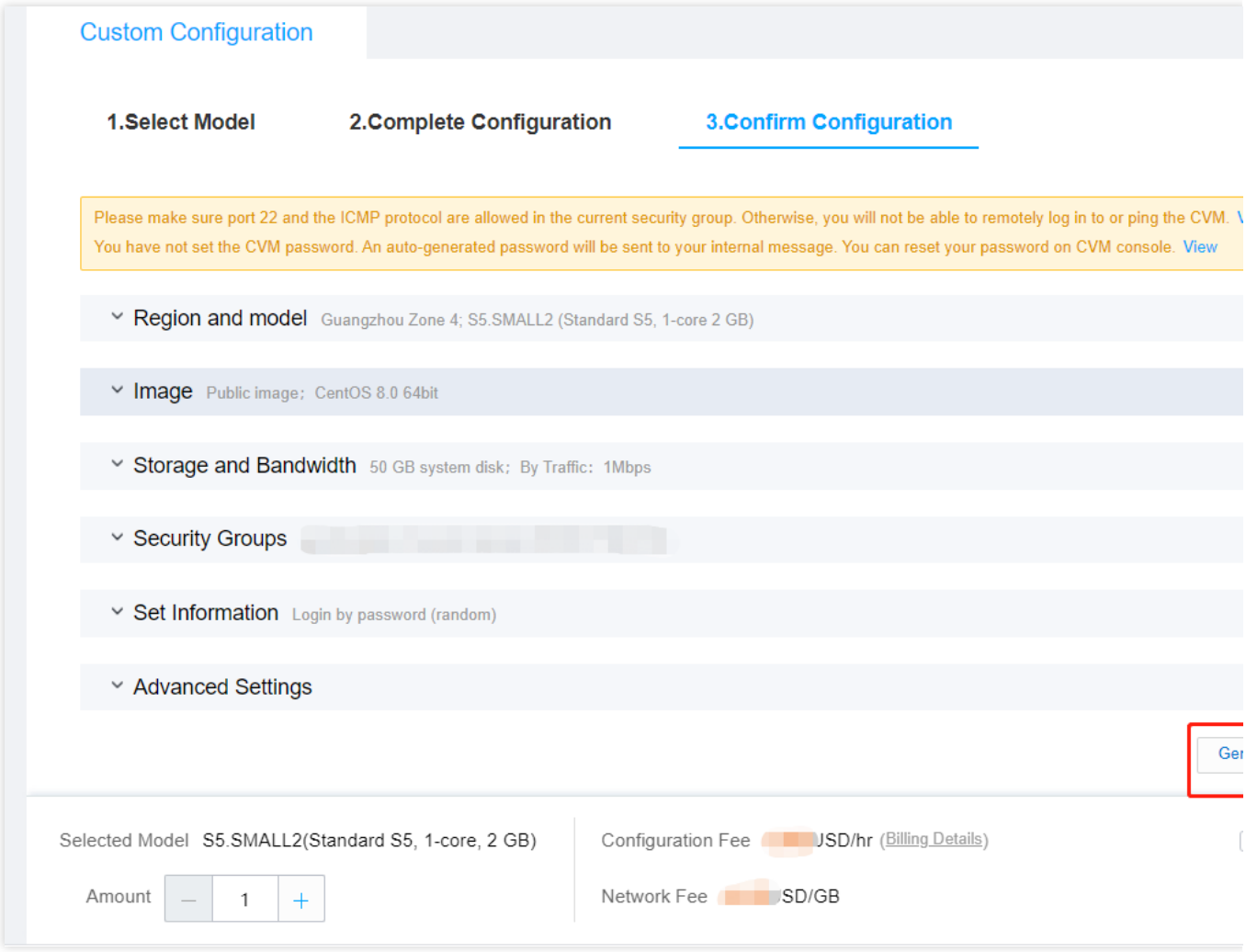
Saat membeli CVM di halaman pembelian CVM, Anda dapat membuat skrip praktik terbaik OpenAPI yang dapat digunakan kembali dengan konfigurasi yang dipilih. Anda kemudian dapat menggunakan kode ini untuk membeli instans CVM dengan konfigurasi yang sama.

## Prasyarat

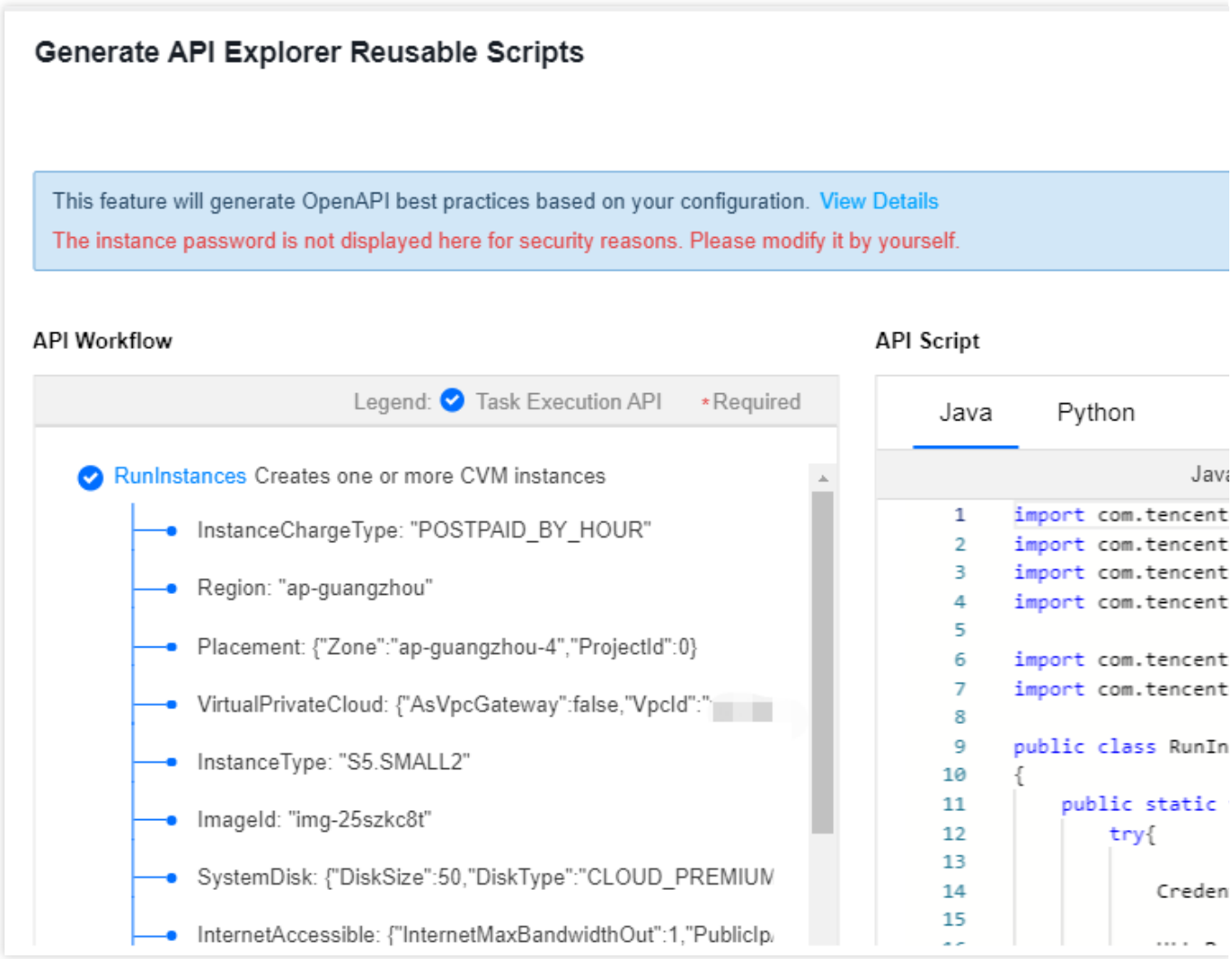
Anda telah login ke konsol Tencent Cloud dan mengakses halaman CVM **Custom Configuration** (Konfigurasi Kustom).
Anda telah menyelesaikan konfigurasi CVM dan masuk ke halaman **Confirm Configuration** (Konfigurasi Kustom).
Untuk mempelajari tentang cara mengonfigurasi parameter, lihat Membuat Instans melalui Halaman Pembelian CVM.

## Petunjuk

1. Pada halaman **Confirm Configuration** (Konfirmasi Konfigurasi), klik **Generate API Explorer Reusable Scripts** (Buat Skrip API Explorer yang Dapat Digunakan Kembali) seperti yang ditunjukkan di bawah ini:




2. Anda dapat melihat informasi berikut di jendela pop-up.




**API Workflow** (Alur Kerja API): memberikan deskripsi dan parameter aktual dari `RunInstances` API berdasarkan konfigurasi yang dipilih. Parameter yang ditandai dengan "*" diperlukan untuk API. Anda dapat mengarahkan kursor ke data untuk menampilkannya sepenuhnya.

**API Script** (Skrip API): menghasilkan kode dalam bahasa pemrograman Java dan Python. Pilih tab Java atau Python sesuai kebutuhan, klik **Copy Script** (Salin Skrip) di sudut kanan atas, dan simpan kode untuk membeli instans CVM yang berisi konfigurasi yang sama.

**Keterangan:**

Kata sandi instans tidak akan ditampilkan pada halaman atau kode skrip untuk alasan keamanan. Harap modifikasinya dengan sendiri.

Tanggal kedaluwarsa kolektif tidak dapat diatur dalam skrip API Explorer yang dapat digunakan kembali. Anda perlu mengaturnya setelah membuat CVM.

# Kelola template startup instans

Waktu update terbaru：2024-03-14 14:42:29

## Skenario pengoperasian

Template startup instans menyimpan informasi konfigurasi yang diperlukan untuk membuat instans Cloud Virtual Machine (CVM) (kecuali kata sandi instans). Anda dapat menggunakan template startup instans yang ditentukan untuk membuat instans dengan cepat, serta meningkatkan efisiensi dan pengalaman pengguna. Artikel ini memperkenalkan cara membuat, mengelola, dan menggunakan template startup instans melalui konsol CVM agar dapat membuat instans dengan cepat.

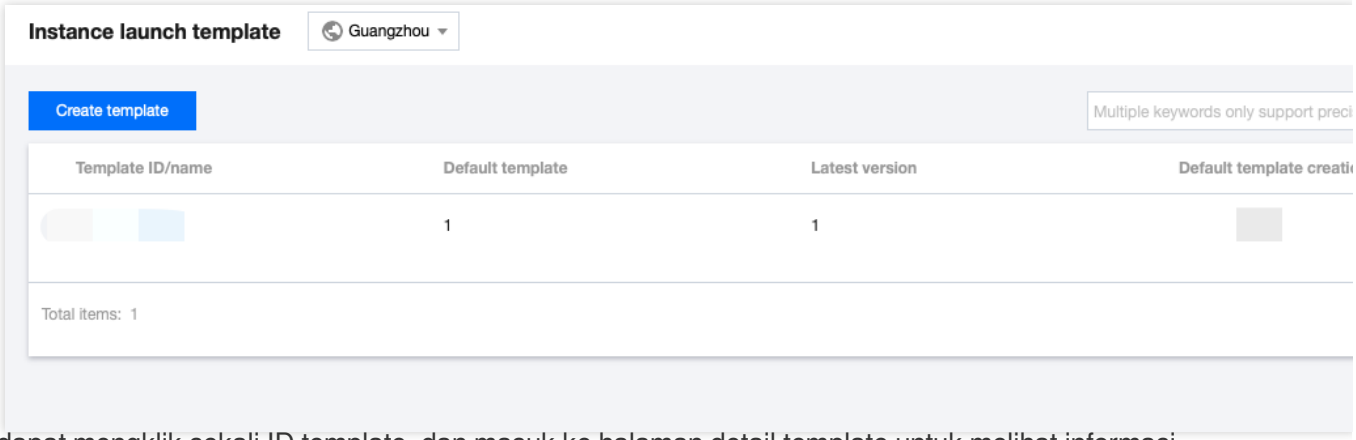
## Petunjuk penggunaan

Modifikasi konfigurasi tidak didukung setelah template startup instans berhasil dibuat.
Template startup instans dapat membuat satu atau beberapa versi, dan setiap versi dapat mengatur informasi konfigurasi yang berbeda. Anda dapat menentukan versi default, dan konfigurasi versi default akan digunakan saat Anda membuat instans dengan template startup instans.

## Langkah-langkah pengoperasian

### Membuat dan melihat template instans

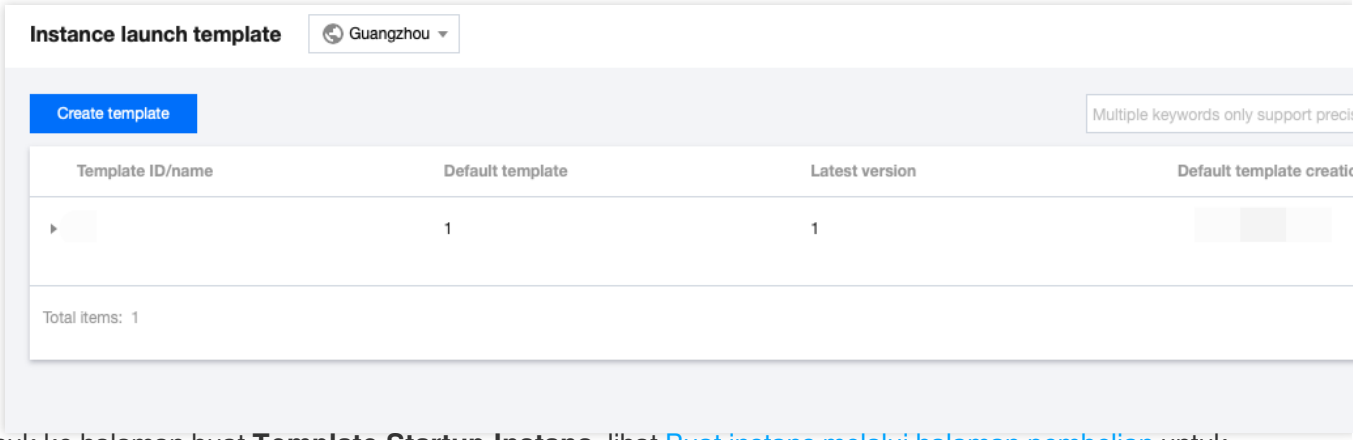
1. Login Konsol CVM, dan pilih **Template Startup Instans** di bilah navigasi kiri.
2. Di halaman **Template Startup Instans**, klik sekali **Template Baru**.
3. Masuk ke halaman buat **Template Startup Instans**, **Nama template**dan**Deskripsi template** dapat dikustomisasi. Untuk konfigurasi lainnya, silakan lihat Buat instans melalui halaman pembelian untuk mengaturnya.
4. Pada langkah **Konfirmasi informasi konfigurasi** , baca dan centang **setuju dengan "Perjanjian Layanan Tencent Cloud"** dan **"Petunjuk Pembelian"** , lalu cukup klik sekali **Buat sekarang** .
Setelah berhasil dibuat, template startup instans dapat dilihat di konsol. Seperti yang ditunjukkan pada gambar di bawah ini:



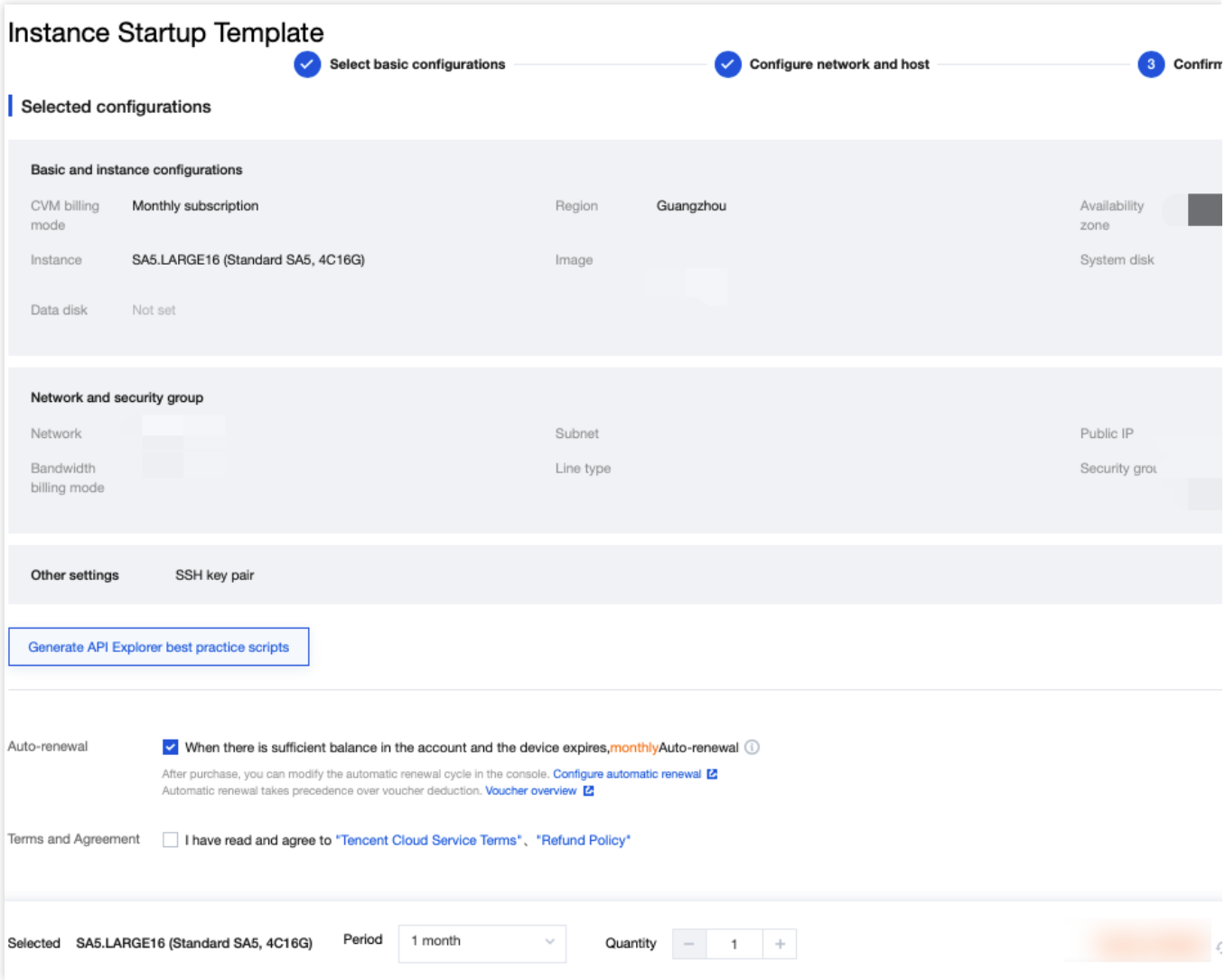

Anda dapat mengklik sekali ID template, dan masuk ke halaman detail template untuk melihat informasi selengkapnya.

## Buat versi template instans

1. Di halaman **Template Startup Instans**, pilih **Versi baru** di sebelah kanan baris yang perlu dibuatkan template versi. Seperti yang ditunjukkan pada gambar di bawah ini:




2. Masuk ke halaman buat **Template Startup Instans**, lihat Buat instans melalui halaman pembelian untuk mengaturnya.
3. Pada langkah **Konfirmasi informasi konfigurasi** , baca dan centang **Setuju dengan "Perjanjian Layanan Tencent Cloud" dan "Petunjuk Pembelian"** .
Anda dapat memilih **Bandingkan konfigurasi sebelumnya**, dan mengonfirmasi perbedaan antara versi baru dan template startup instans sebelumnya di jendela pop-up "Bandingkan konfigurasi sebelumnya". Seperti yang ditunjukkan pada gambar di bawah ini:




4. Setelah mengonfirmasi keakuratannya, cukup klik sekali **Buat sekarang**.

Setelah berhasil dibuat, Anda dapat mengklik

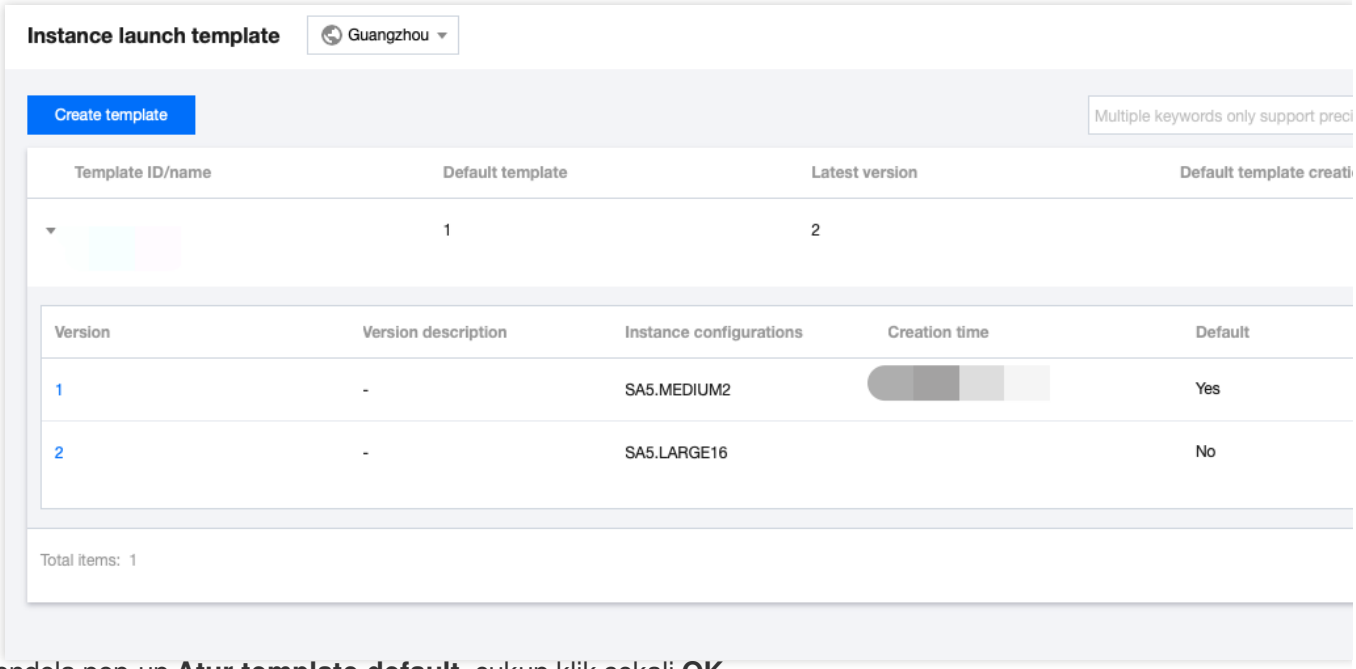
di depan baris template pada halaman **Template Startup Instans**, dan lihat versinya dalam daftar yang diperluas.

## Tentukan versi default dari template instans

1. Di halaman **Template Startup Instans**, klik sekali

di depan baris lokasi template.

2. Dalam daftar yang diperluas, klik sekali **Atur menjadi Default** di sebelah kanan versi yang ingin diatur. Seperti yang ditunjukkan pada gambar di bawah ini:




3. Di jendela pop-up **Atur template default**, cukup klik sekali **OK**.

### Buat instans dengan template instans

1. Di halaman **Template Startup Instans**, pilih **Buat Instans** di sebelah kanan baris lokasi template.

**Keterangan:**

Secara default, konfigurasi template startup instans **versi default** akan digunakan saat membuat instans. Anda juga dapat mengklik sekali

di depan baris lokasi template, dan dalam daftar yang diperluas, pilih versi lain untuk membuat instans.

2. Pada langkah **Konfirmasi informasi konfigurasi** di halaman buat **CVM**, Anda dapat memilih **Bandingkan konfigurasi sebelumnya**, dan mengonfirmasi perbedaan antara instans dan template startup instans di jendela pop-up **Bandingkan konfigurasi sebelumnya**.

3. Setelah mengonfirmasi keakuratannya, baca dan centang **Setuju dengan "Perjanjian Layanan Tencent Cloud"** dan **"Petunjuk Pembelian" , lalu cukup** klik sekali **Aktifkan** .

### Hapus template startup instans

1. Di halaman **Template startup instans**, pilih **Hapus** di sebelah kanan baris lokasi template startup instans yang perlu dihapus.

2. Di jendela pop-up **Hapus**, cukup klik sekali **OK**.

## Dokumen terkait

Buat instans melalui halaman pembelian

# Penamaan Sekuensial Batch atau Penamaan Berbasis String Pola

Waktu update terbaru：2021-12-13 17:07:03

## Skenario

Untuk memungkinkan Anda memberi nama instans CVM yang dibuat secara batch sesuai dengan aturan selama pembuatan, fitur berakhiran menaik secara otomatis dan menentukan string pola yang disediakan.
Saat Anda perlu membeli n instans dan membuat nama instans dalam bentuk tertentu, seperti “CVM+Sequence number” (misalnya, CVM 1, CVM 2, dan CVM 3), Anda dapat menggunakan fitur Secara Otomatis Menaikkan Nomor Berakhiran.
Saat Anda perlu membuat instans **n** (n) dan memberi nama instans tertentu dengan nomor menaik mulai dari **x** (x), Anda dapat menggunakan fitur Menentukan Satu String Pola.
Saat Anda perlu membuat n instans dengan beberapa awalan dalam namanya, yang masing-masing berisi nomor seri tertentu, Anda dapat menggunakan fitur Menentukan Beberapa String Pola.

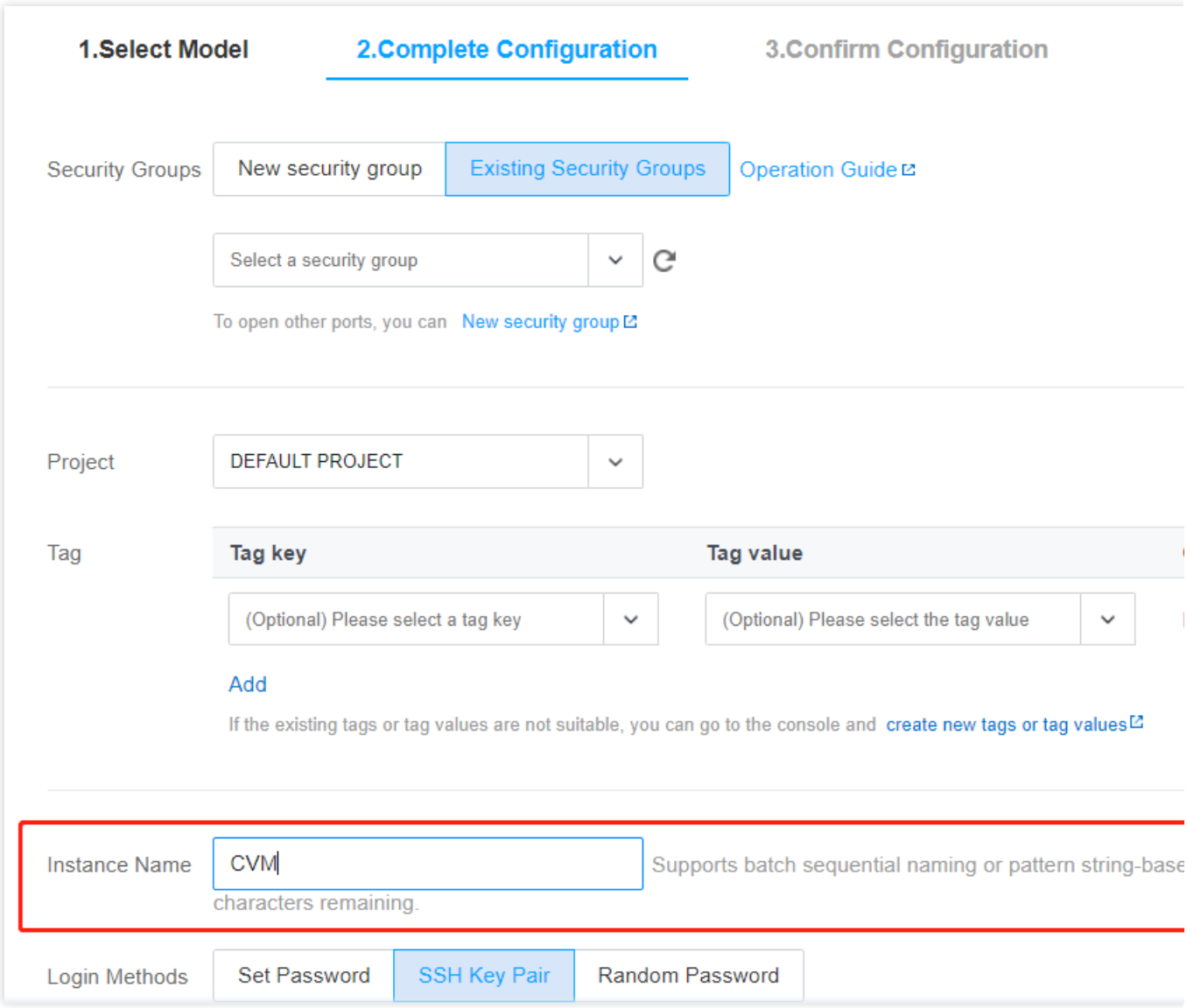
## Langkah-Langkah

### Secara Otomatis Menaikkan Angka Berakhiran

Fitur ini memungkinkan Anda memberi nama instans yang dibeli secara batch dengan awalan yang sama dan nomor berakhiran yang naik secara otomatis.
**Keterangan:**
Instans yang dibuat diberi akhiran dengan angka mulai dari 1 secara default. Nomor berakhiran awal adalah tetap. Contoh berikut mengasumsikan bahwa Anda telah membeli tiga instans dan ingin memberi nama instans tersebut dalam bentuk “CVM+Nomor urut” (misalnya, CVM 1, CVM 2, dan CVM 3).

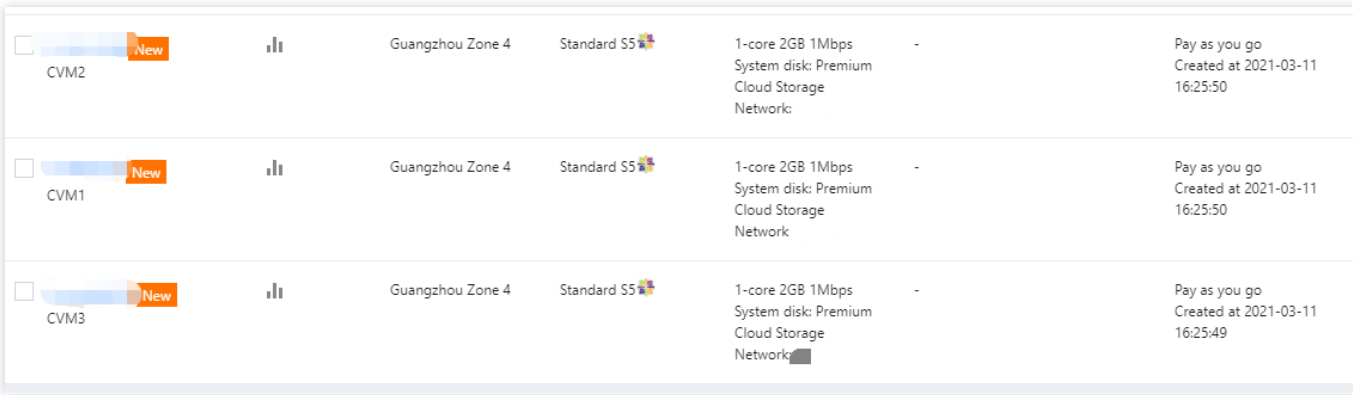
#### Operasi pada Halaman Pembelian

1. Beli tiga instans dengan merujuk ke Buat Instans. Pada halaman tab **2. Security Group and CVM** (2. Grup Keamanan dan CVM), masukkan nama instans berupa **Prefix+Sequence number** (Awalan+Nomor urut). Dalam hal ini, masukkan `CVM` sebagai nama instans.




2. Ikuti petunjuk di halaman dan selesaikan pembayaran.

3. Kembali ke Konsol CVM untuk melihat instans yang baru dibeli. Anda dapat melihat bahwa instans yang dibeli secara batch ini diberi nama dengan awalan yang sama dan nomor akhiran menaik.



#### Operasi API

Di RunInstances API, atur bidang InstanceName ke `CVM` .

### Menentukan String Pola

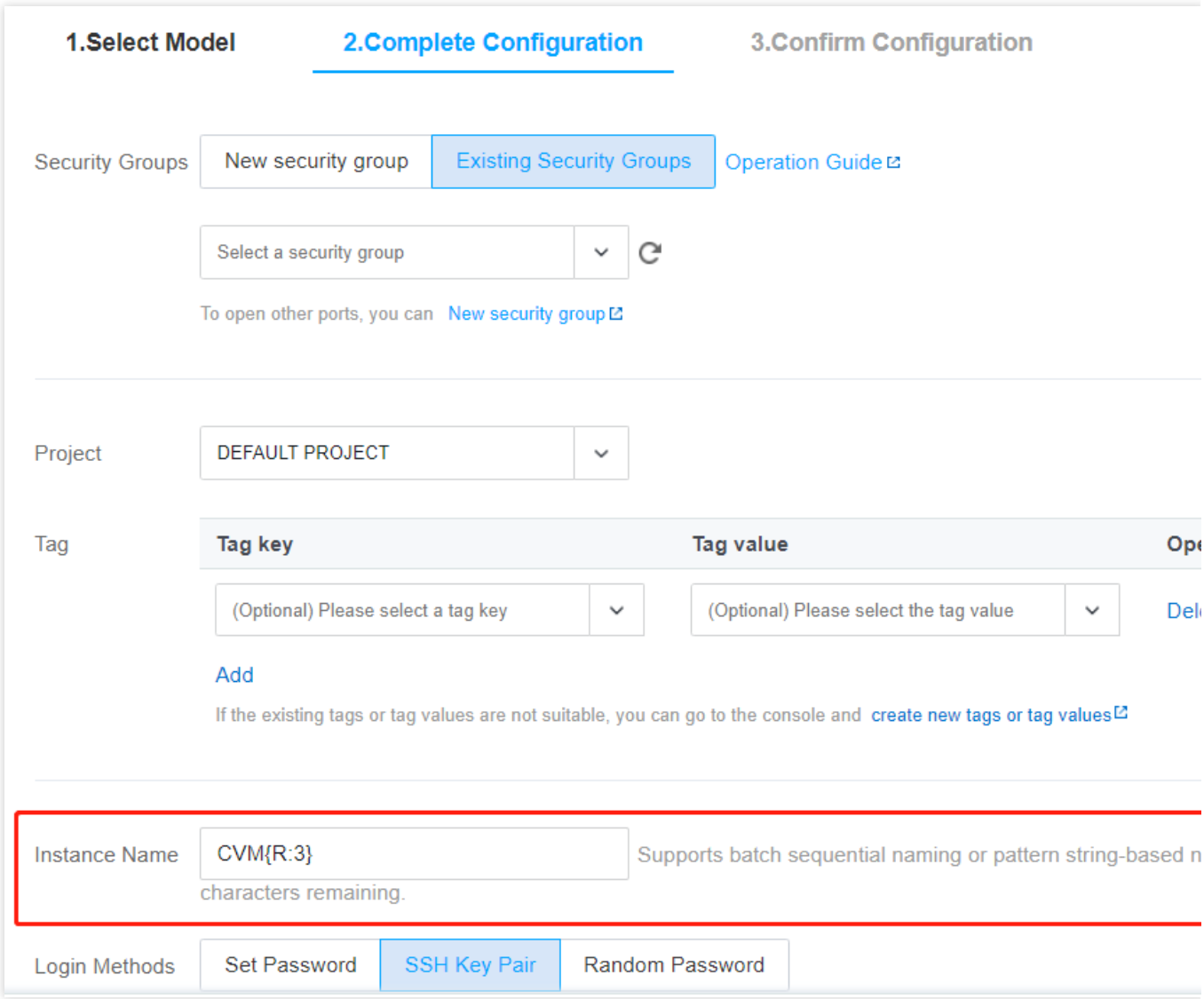
Fitur ini memungkinkan Anda memberi nama instans yang dibeli secara batch dalam bentuk kompleks dengan nomor seri tertentu. Anda dapat menggunakan satu atau beberapa string pola dalam nama instans sesuai kebutuhan. Nama instans dengan string pola yang ditentukan dalam bentuk **{R:x}** ({R:x}), di mana **x** (x) menunjukkan nomor awal dalam nama instans yang dihasilkan.

#### Menentukan Satu String Pola

Contoh berikut mengasumsikan bahwa Anda ingin membuat tiga instans dan menamainya dengan nomor menaik mulai dari 3.

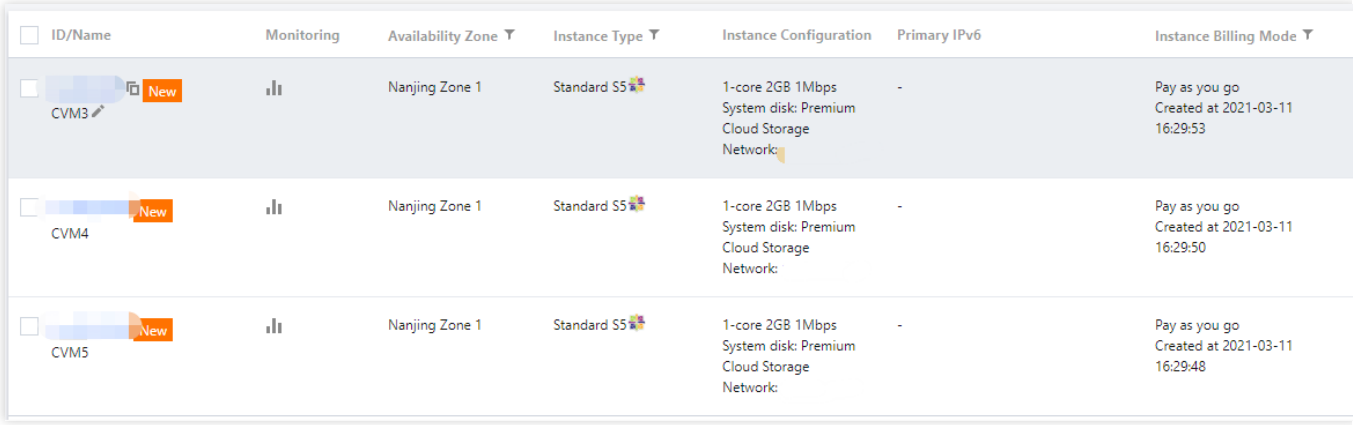
##### Operasi pada Halaman Pembelian

1. Beli tiga instans dengan merujuk ke Buat Instans. Pada halaman tab **2. Set the CVM** (2. Atur CVM), masukkan nama instans berupa **Prefix+Specified pattern string {R:x}** (Prefix+Specified pattern string {R:x}). Dalam hal ini, masukkan `CVM{R:3}` sebagai nama instans.




2. Ikuti petunjuk di halaman dan selesaikan pembayaran.

3. Kembali ke Konsol CVM untuk melihat instans yang baru dibeli. Anda dapat melihat bahwa instans yang dibeli secara batch ini diberi nama dengan awalan yang sama dan nomor berakhiran menaik mulai dari 3.



#### Operasi API

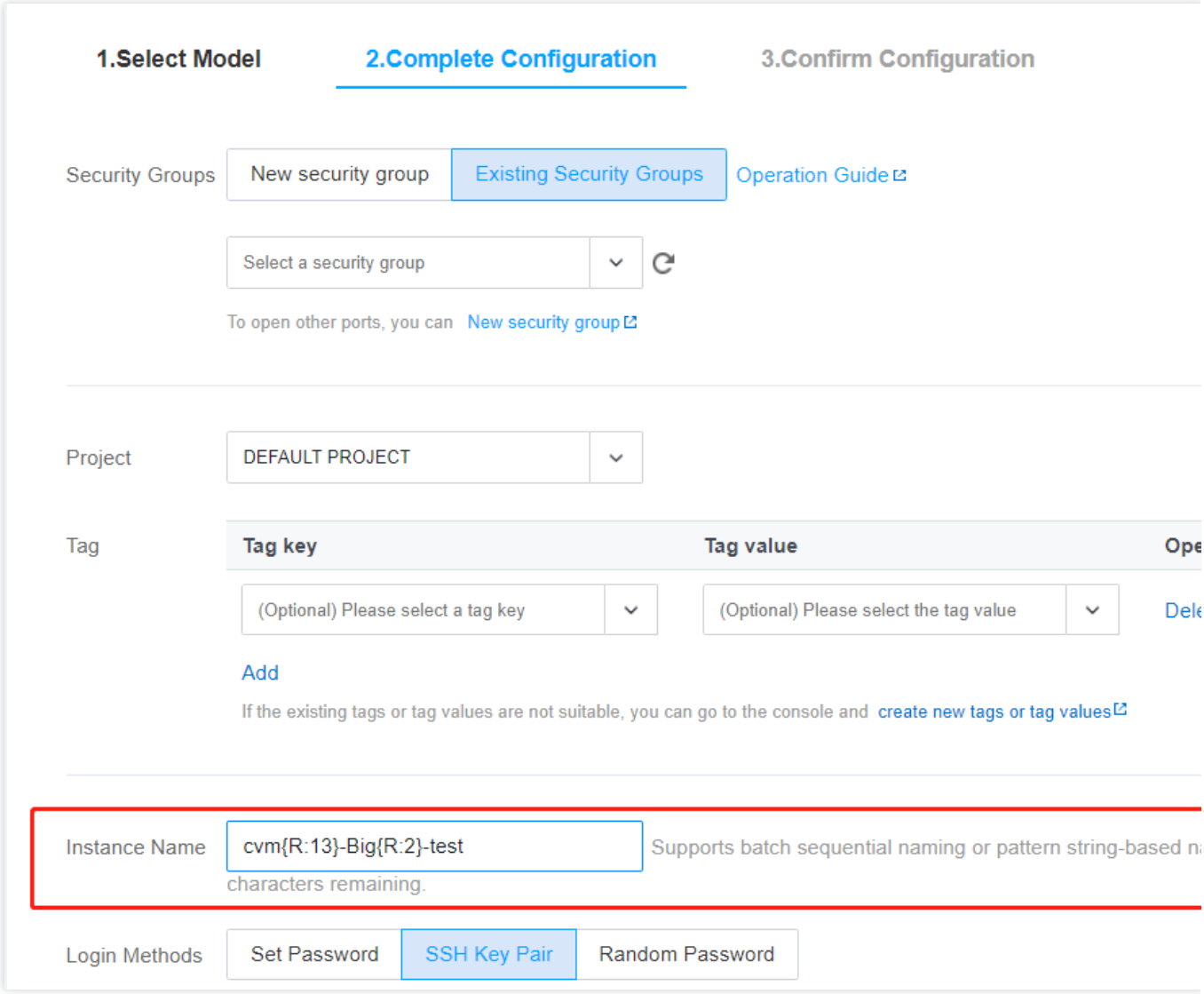
Di RunInstances API, atur kolom InstanceName ke `CVM{R:3}` .

### Menentukan Beberapa String Pola

Contoh berikut mengasumsikan bahwa Anda ingin membuat tiga instans dan memberinya nama dengan awalan **cvm** (cvm), **Big** (Big), dan **test** (test), dengan **cvm** (cvm) dan **Big** (Big) masing-masing diikuti dengan nomor menaik mulai dari 13 dan 2. Misalnya, namanya masing-masing adalah cvm13-Big2-test, cvm14-Big3-test, dan cvm15-Big4-test.

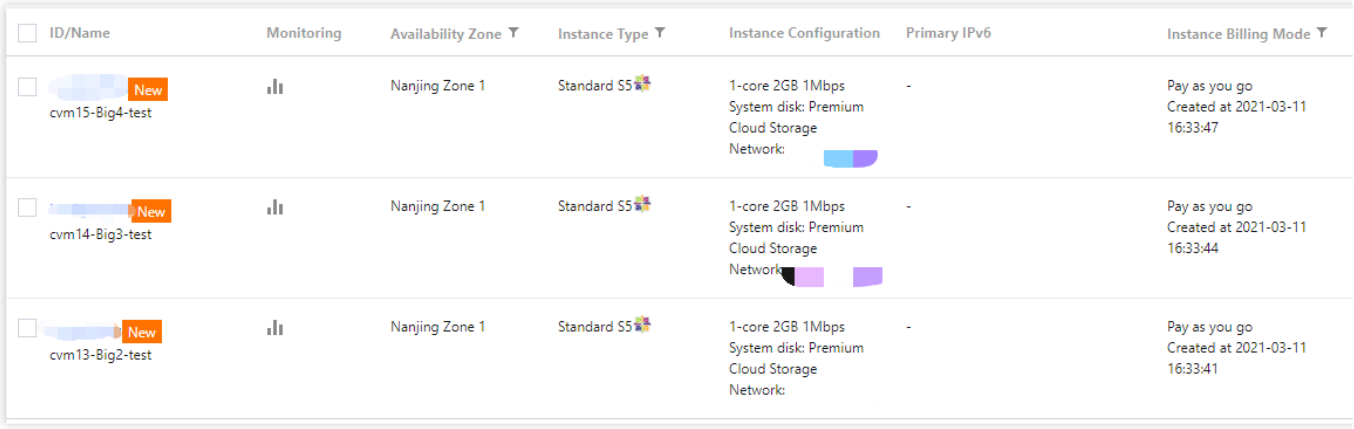
#### Operasi pada Halaman Pembelian

1. Beli tiga instans dengan merujuk ke Buat Instans. Pada halaman tab **2. Set the CVM** (2. Atur CVM), masukkan nama instans berupa **Prefix+Specified pattern string {R:x}-Prefix+Specified pattern string {R:x}-Prefix** (Prefix+Specified pattern string {R:x}-Prefix+Specified pattern string {R:x}-Prefix). Dalam hal ini, masukkan `cvm{R:13}-Big{R:2}-test` sebagai nama instans.




2. Ikuti petunjuk di halaman dan selesaikan pembayaran.

3. Kembali ke Konsol CVM untuk melihat instans yang baru dibeli. Anda dapat melihat bahwa instans yang dibeli secara batch ini diberi nama dengan awalan diikuti dengan nomor menaik mulai dari nomor yang ditentukan.




**Operasi API**

Di RunInstances API, atur bidang InstanceName ke `cvm{R:13}-Big{R:2}-test` .

# Login ke Instans Linux
# Login ke Instans Windows Menggunakan RDP (Direkomendasikan)

Waktu update terbaru：2021-12-13 17:07:06

### Skenario

WebShell adalah metode login yang direkomendasikan oleh Tencent Cloud. Meskipun OS lokal Anda adalah Windows, Linux, atau Mac OS, selama Anda telah membeli IP publik untuk instans, Anda dapat login melalui Web Shell. Dokumen ini menjelaskan cara login ke instans Linux melalui Web Shell.
Manfaat Web Shell:
Mendukung operasi salin dan tempel dengan tombol pintas.
Mendukung pengguliran dengan roda mouse.
Mendukung masukan bahasa Mandarin.
Fitur keamanan yang tinggi (kata sandi atau kunci diperlukan untuk setiap login).

## OS Lokal yang Berlaku

Windows, Linux, atau MacOS.

## Metode Autentikasi

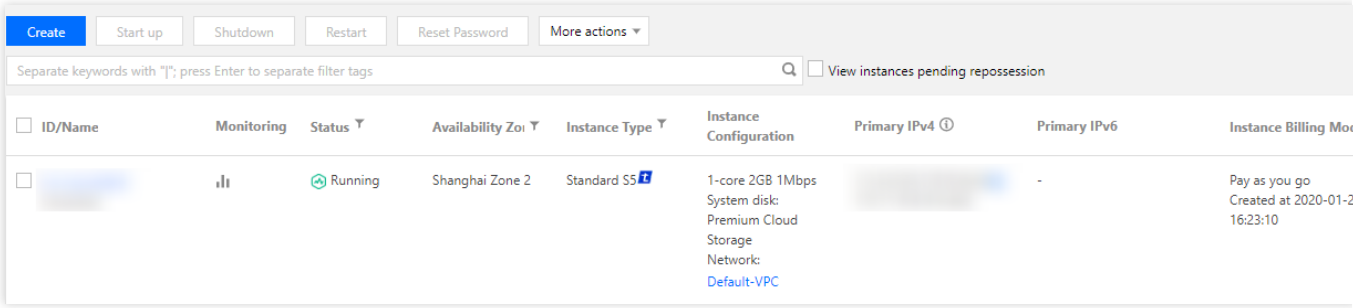
**Password** (Kata Sandi) atau **Key** (Kunci)

## Prasyarat

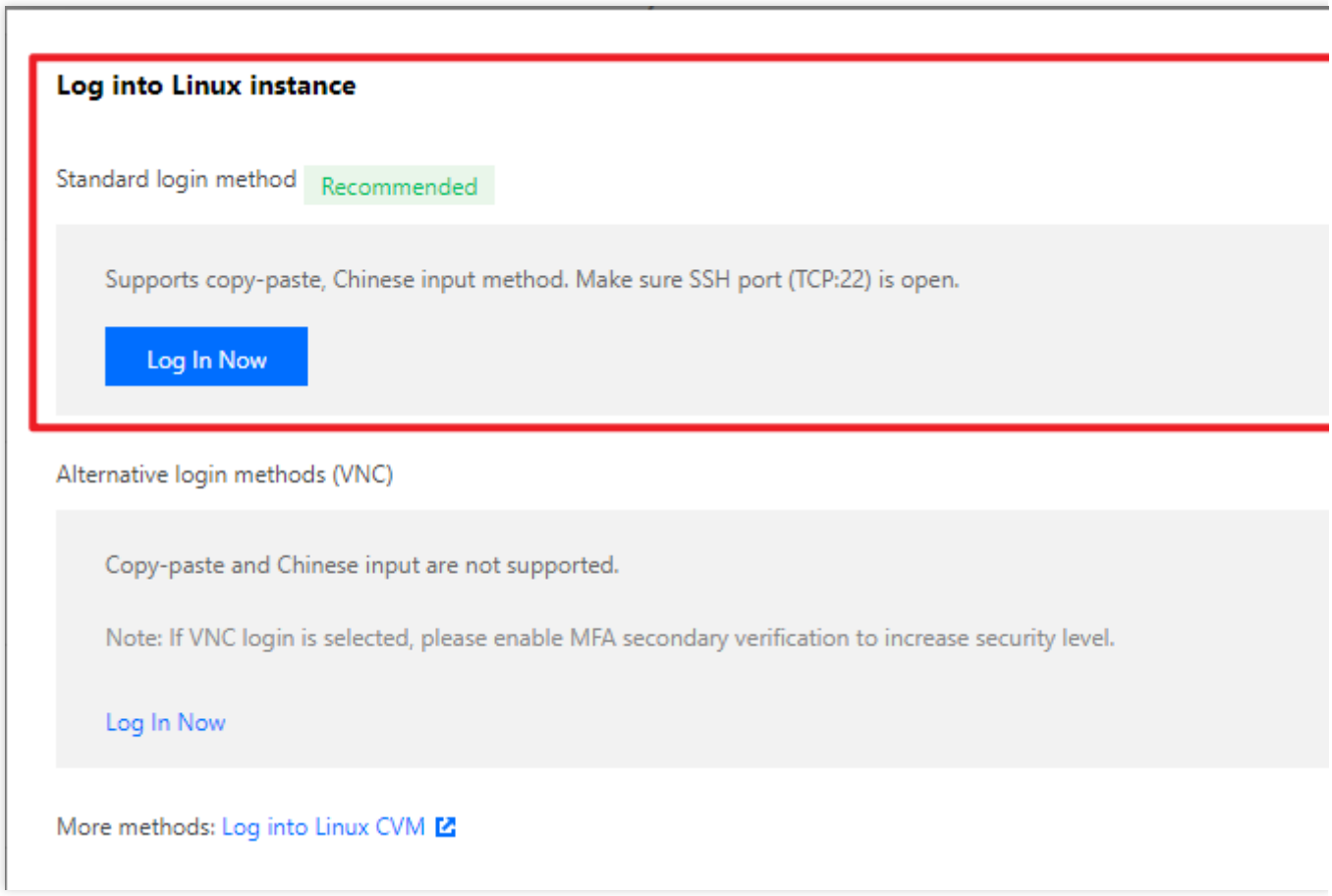
Anda harus sudah memiliki akun admin dan kata sandi (atau kunci) untuk instans yang digunakan untuk login.
Jika Anda memilih **Random Password** (Kata Sandi Acak) saat membuat instans, buka Pesan Internal untuk memeriksa kata sandi.
Jika lupa kata sandi Anda, atur ulang kata sandi instans.
Pastikan instans CVM memiliki IP publik, dan port 22 terbuka (jika CVM dibeli dengan “Konfigurasi Cepat”, port ini terbuka secara default.)

### Petunjuk

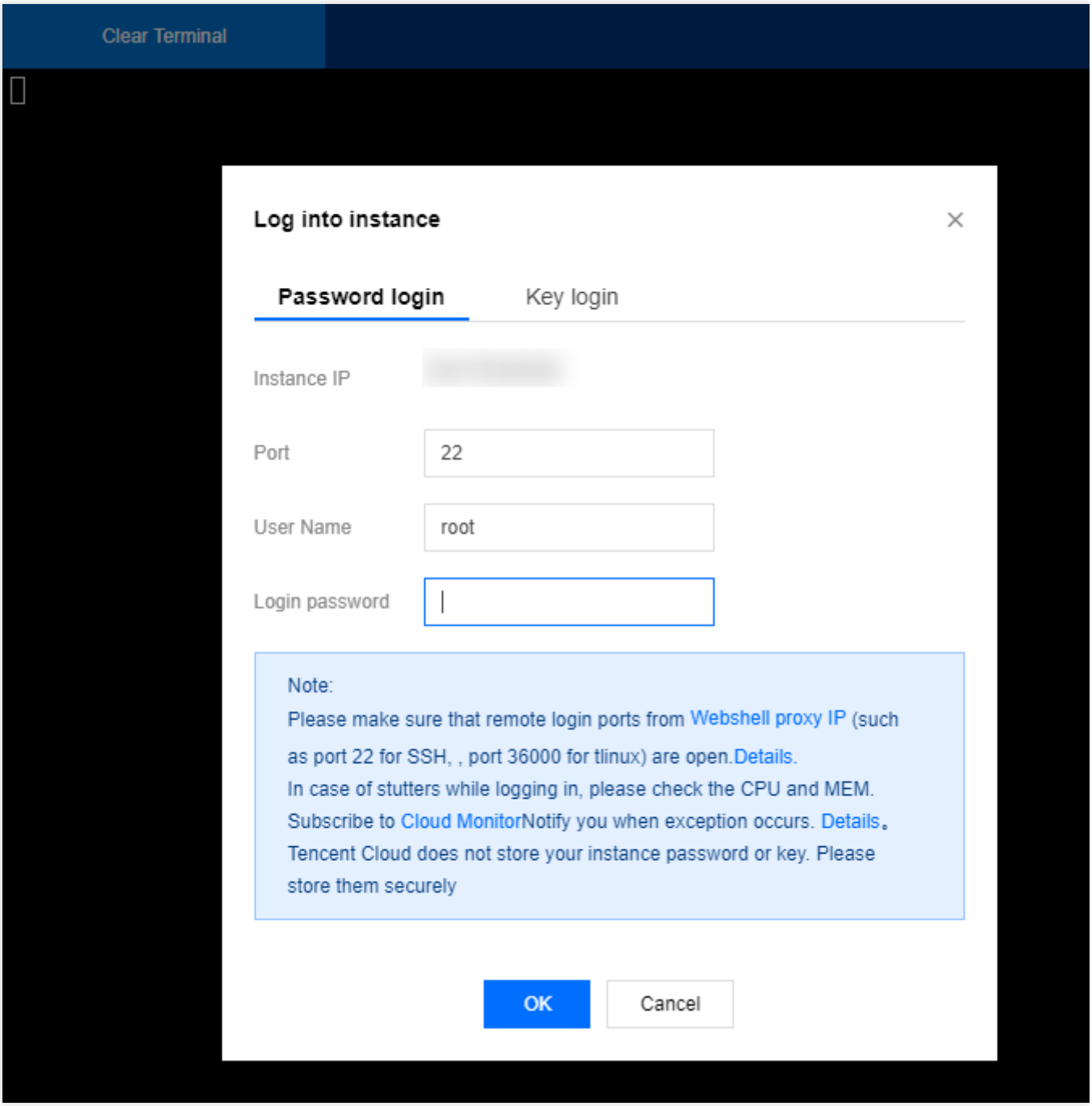
1. Login ke Konsol CVM.
2. Pada halaman manajemen instans, pilih CVM Linux tempat Anda ingin login, lalu klik **Log In** (Login), seperti yang ditunjukkan di bawah ini:



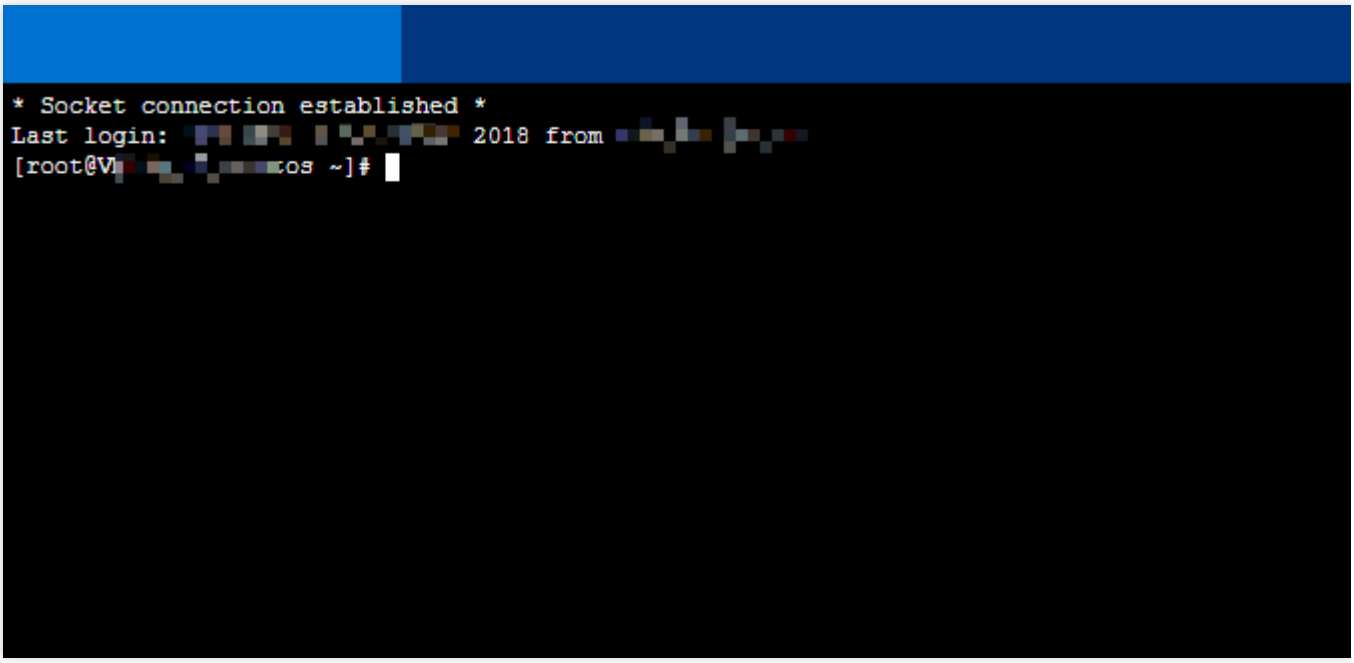

3. Di jendela pop-up **Log into Linux Instance** (Login ke Instans Linux), pilih **Standard login method** (Metode login standar), lalu klik **Log In Now** (Login Sekarang), seperti yang ditunjukkan di bawah ini.




4. Di jendela **Log into Instance** (Login ke Instans), pilih **Password Login** (Login Kata Sandi) atau **Key Login** (Login Kunci), seperti yang ditunjukkan di bawah ini:




Jika login berhasil, “Socket connection established” (Koneksi soket dibuat) akan muncul seperti yang ditampilkan di bawah ini:




## Operasi Selanjutnya

Setelah login ke CVM, Anda dapat membangun situs web atau forum pribadi di Tencent Cloud CVM atau melakukan operasi lain. Untuk informasi selengkapnya, lihat dokumen berikut: Membuat situs WordPress pribadi.

# Login ke Instans Linux melalui Fitur Login Jarak Jauh

Waktu update terbaru：2021-12-13 17:07:06

## Ikhtisar

Dokumen ini mengambil PuTTY sebagai contoh untuk menjelaskan cara login ke instans Linux dari Windows menggunakan perangkat lunak login jarak jauh.

## OS yang Berlaku

Windows

## Metode Autentikasi

**Password** (Kata Sandi) atau **Key** (Kunci)

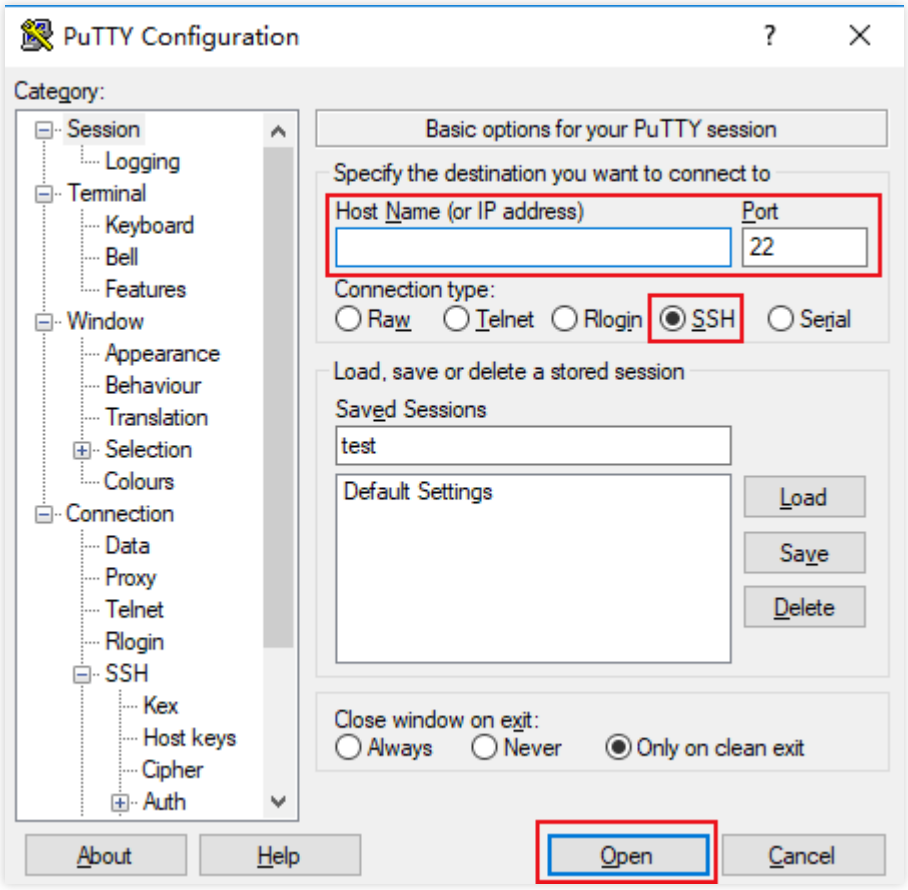
## Prasyarat

Anda harus sudah memiliki akun admin dan kata sandi (atau kunci) untuk login ke instans.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, buka Pusat Pesan untuk mendapatkan kata sandi terlebih dahulu.
Jika lupa kata sandi Anda, harap atur ulang kata sandi instans Anda.
IP publik telah dibeli dan diperoleh untuk instans CVM Anda, dan port 22 terbuka (ini terbuka secara default untuk CVM yang dibeli dengan konfigurasi cepat).

## Petunjuk

Logging in with a password
Logging in with a key
1. Unduh perangkat lunak login jarak jauh Windows, yaitu PuTTY.
2. Klik dua kali **putty.exe** (putty.exe) untuk membuka klien PuTTY.

3. Di jendela **PuTTY Configuration** (Konfigurasi PuTTY), masukkan konten berikut, seperti yang ditunjukkan di bawah ini:




Konfigurasikan parameter sebagai berikut:

**Host Name (or IP address)** (Nama Host (atau alamat IP)): IP publik untuk CVM. Login ke Konsol CVM untuk mendapatkan IP publik dari daftar instans dan halaman detail.

**Port** (Port): port CVM, yang harus “22”.

**Connection type** (Jenis koneksi): pilih **SSH** (SSH).

**Saved Sessions** (Sesi Tersimpan): masukkan nama sesi, seperti `test` .

Setelah mengonfigurasi **Host Name** (Nama Host), konfigurasikan dan simpan **Saved Sessions** (Sesi Tersimpan). Anda dapat mengklik dua kali nama sesi yang disimpan di bawah **Saved Sessions** (Sesi Tersimpan) untuk login ke CVM.

4. Klik **Open** (Buka) untuk masuk ke antarmuka **PuTTY** (PuTTY). Command prompt **login as:** (login sebagai:) akan muncul.

5. Masukkan nama pengguna setelah **login as:** (login sebagai:), lalu tekan **Enter** (Enter).

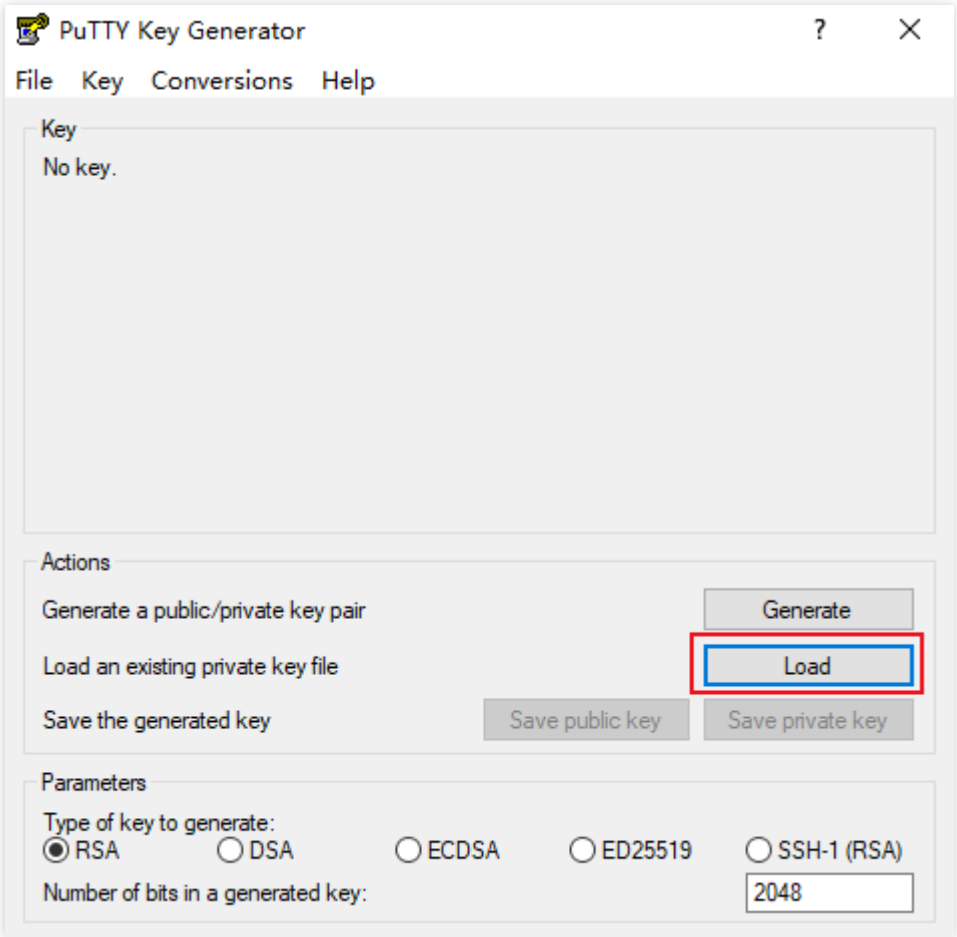
6. Masukkan kata sandi setelah **Password** (Kata Sandi), lalu tekan **Enter** (Enter).

Kata sandi yang dimasukkan tidak ditampilkan secara default, seperti yang ditunjukkan di bawah ini:


Setelah login, Anda dapat melihat informasi tentang CVM tempat Anda masuk saat ini di sebelah kiri command prompt.

1. Unduh perangkat lunak login jarak jauh Windows, yaitu PuTTY. Baik putty.exe dan puttygen.exe diperlukan.
2. Klik dua kali **puttygen.exe** (puttygen.exe) untuk membuka klien Putty Key.
3. Klik **Load** (Muat), pilih dan akses jalur penyimpanan kunci pribadi yang diunduh. Anda harus mengunduh dan menyimpan kunci pribadi Anda setelah membuat pasangan kunci. Untuk informasi selengkapnya, lihat Mengelola Kunci SSH

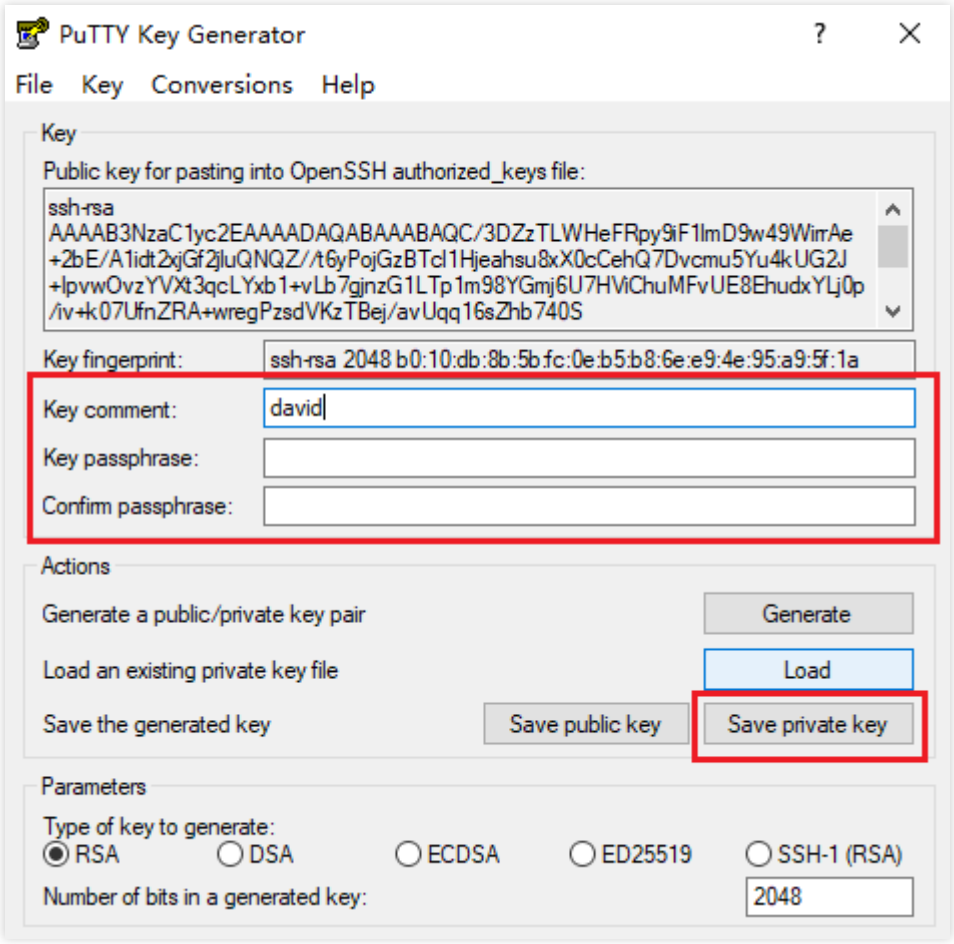
Misalnya, pilih dan buka file kunci pribadi `david` , seperti yang ditunjukkan di bawah ini:



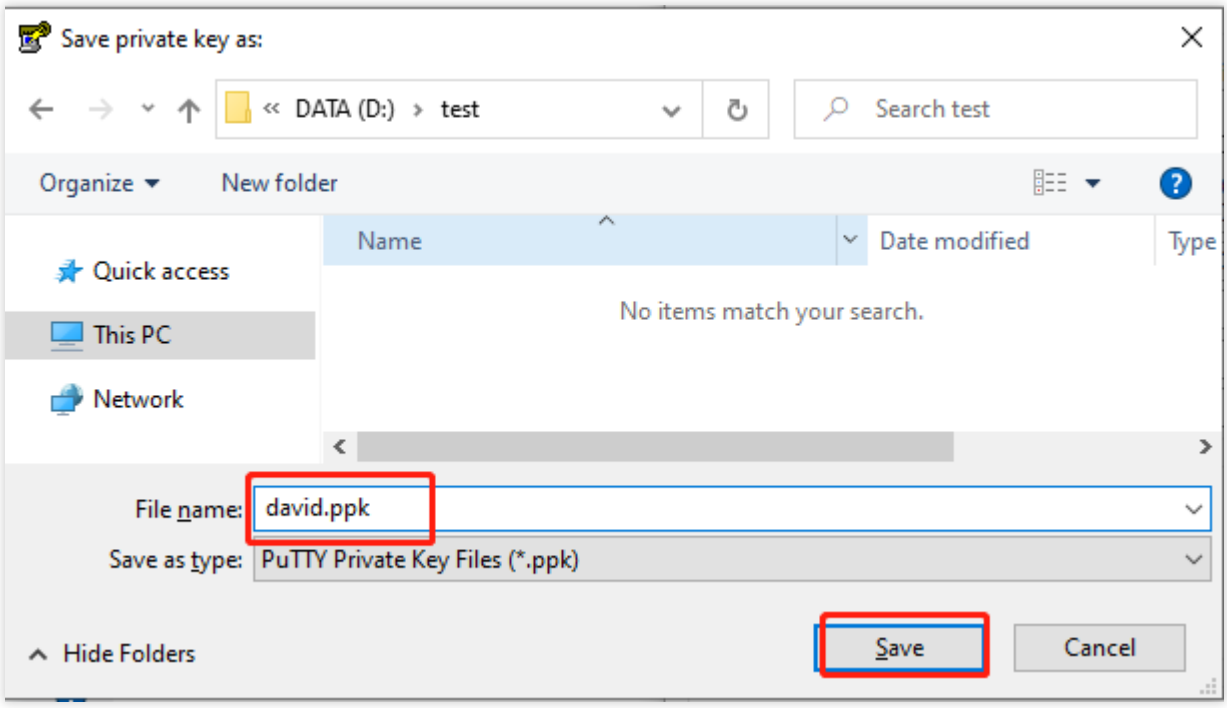

4.

Di jendela **PuTTY Key Generator**

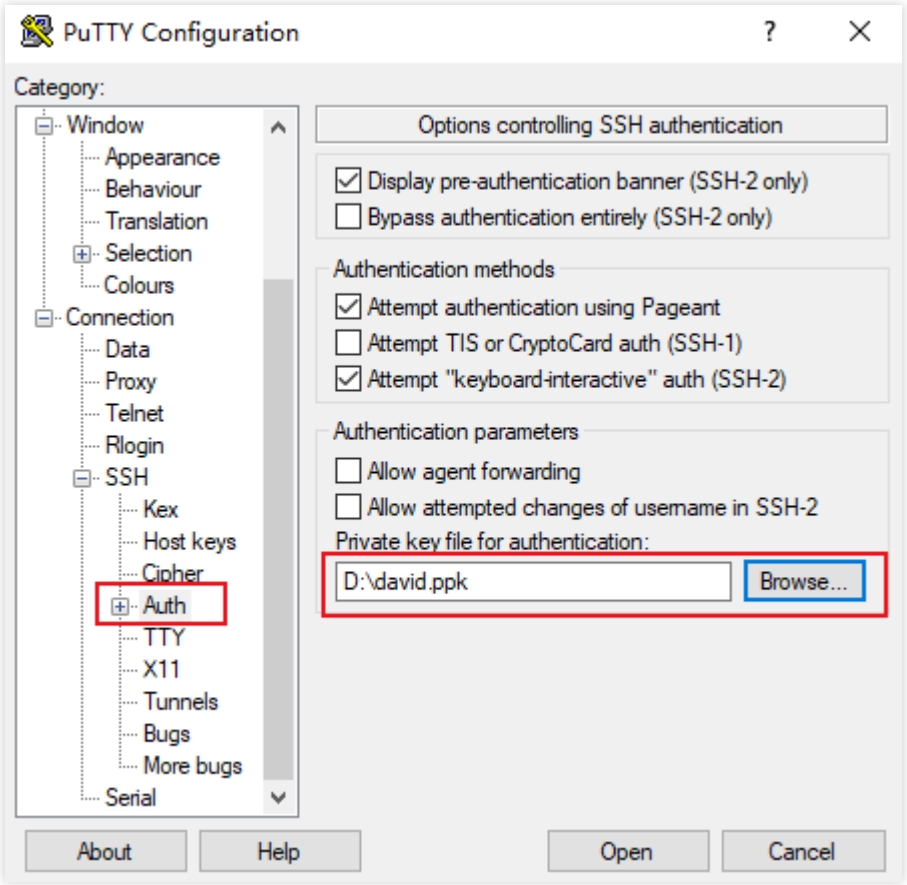
(Pembuat Kunci PuTTY), masukkan nama kunci dan kata sandi kunci pribadi terenkripsi (opsional), dan klik **Save private key** (Simpan kunci pribadi), seperti yang ditunjukkan di bawah ini:



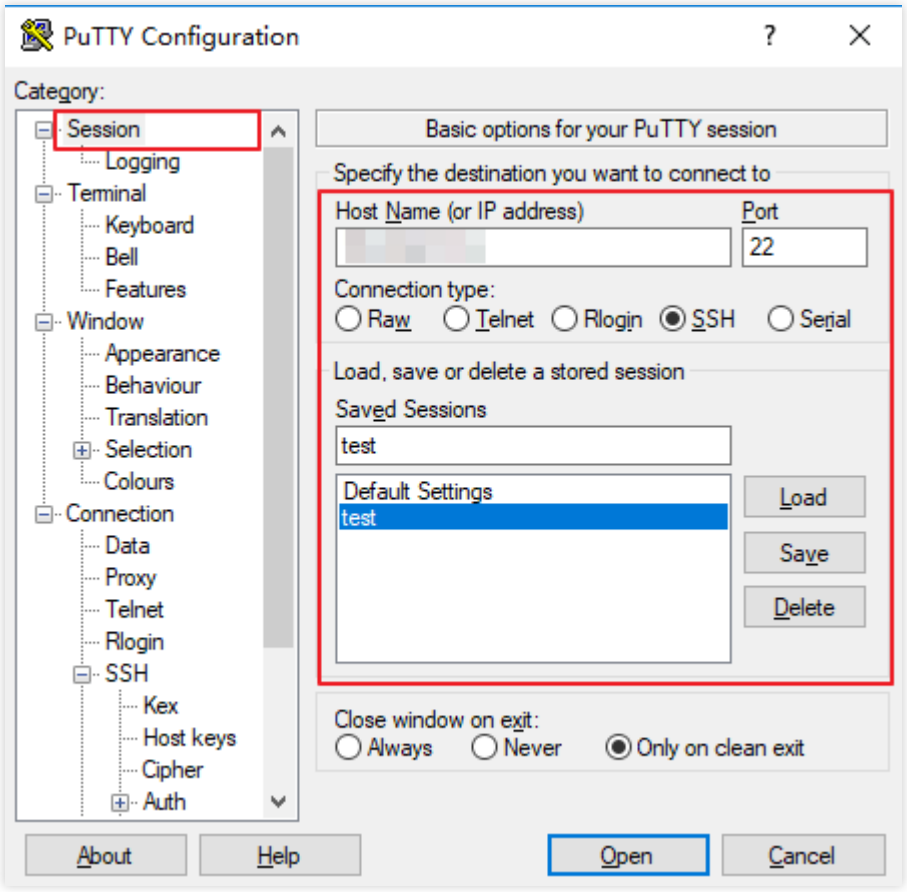

5. Di jendela pop-up, pilih jalur tempat kunci akan disimpan. Di bidang **File name** (Nama file), masukkan “Key Name.ppk”, lalu klik **Save** (Simpan). Misalnya, simpan file kunci pribadi `david` sebagai `david.ppk`, seperti yang ditunjukkan di bawah ini:




6. Klik dua kali **putty.exe** (putty.exe) untuk membuka klien PuTTY.
7. Di bilah sisi kiri, buka **Connection** (Koneksi) > **SSH** (SSH) > **Auth** (Auth), lalu masuk ke antarmuka konfigurasi **Auth** (Auth).
8. Klik **Browse** (Jelajahi), lalu pilih dan akses jalur tempat kunci disimpan, seperti yang ditunjukkan di bawah ini:




9. Beralih ke antarmuka konfigurasi **Session** (Sesi). Konfigurasikan CVM IP, port, dan jenis koneksi, seperti yang ditunjukkan di bawah ini:




**Host Name (or IP address)** (Nama Host (atau alamat IP)): IP publik untuk CVM. Login ke Konsol CVM untuk mendapatkan IP publik dari daftar instans dan halaman detail.

**Port** (Port): port CVM, yang harus “22”.

**Connection type** (Jenis koneksi): pilih **SSH** (SSH).

**Saved Sessions** (Sesi Tersimpan): masukkan nama sesi, seperti `test` .

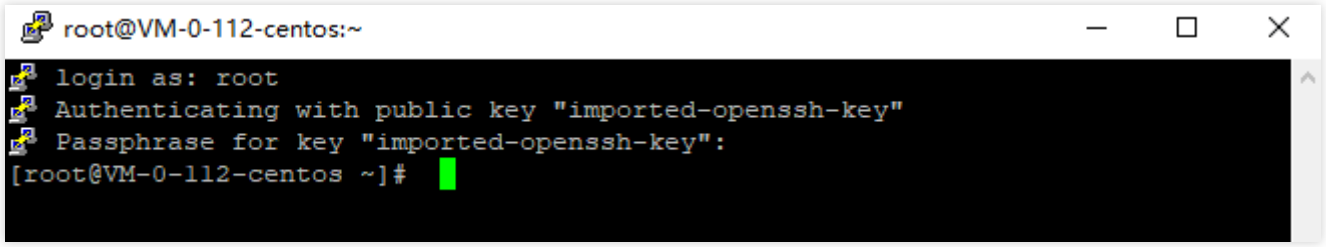
Setelah mengonfigurasi **Host Name** (Nama Host), konfigurasikan dan simpan **Saved Sessions** (Sesi Tersimpan). Anda dapat mengklik dua kali nama sesi yang disimpan di bawah **Saved Sessions** (Sesi Tersimpan) untuk login ke CVM.

10. Klik **Open** (Buka) untuk masuk ke antarmuka **PuTTY** (PuTTY). Command prompt **login as:** (login sebagai:) akan muncul.

11. Masukkan nama pengguna setelah **login as:** (login sebagai:), lalu tekan **Enter** (Enter).

12. Masukkan kata sandi yang dikonfigurasi di Langkah 4 setelah **Passphrase for key "imported-openssh-key":** (Frasa sandi untuk kunci "imported-openssh-key":), lalu tekan **Enter** (Enter).

Kata sandi yang dimasukkan tidak ditampilkan secara default, seperti yang ditunjukkan di bawah ini:




Setelah login, Anda dapat melihat informasi tentang CVM tempat Anda masuk saat ini di sebelah kiri command prompt.

## Operasi Selanjutnya

Setelah login ke CVM, Anda dapat membangun situs web atau forum pribadi atau melakukan operasi lain. Untuk informasi selengkapnya, lihat:

Menyiapkan WordPress

Membuat Forum Discuz!

# Login ke Instans Linux melalui Kunci SSH

Waktu update terbaru：2021-12-13 17:07:06

## Ikhtisar

Dokumen ini menjelaskan cara menggunakan kunci SSH untuk login ke instans Linux dari Linux, Mac OS, atau Windows lokal.

## Sistem yang Didukung

Linux, Mac OS, atau Windows (termasuk Windows 10 dan Windows Server 2019)

## Metode Autentikasi

**Password** (Kata Sandi) atau **Key** (Kunci)

## Prasyarat

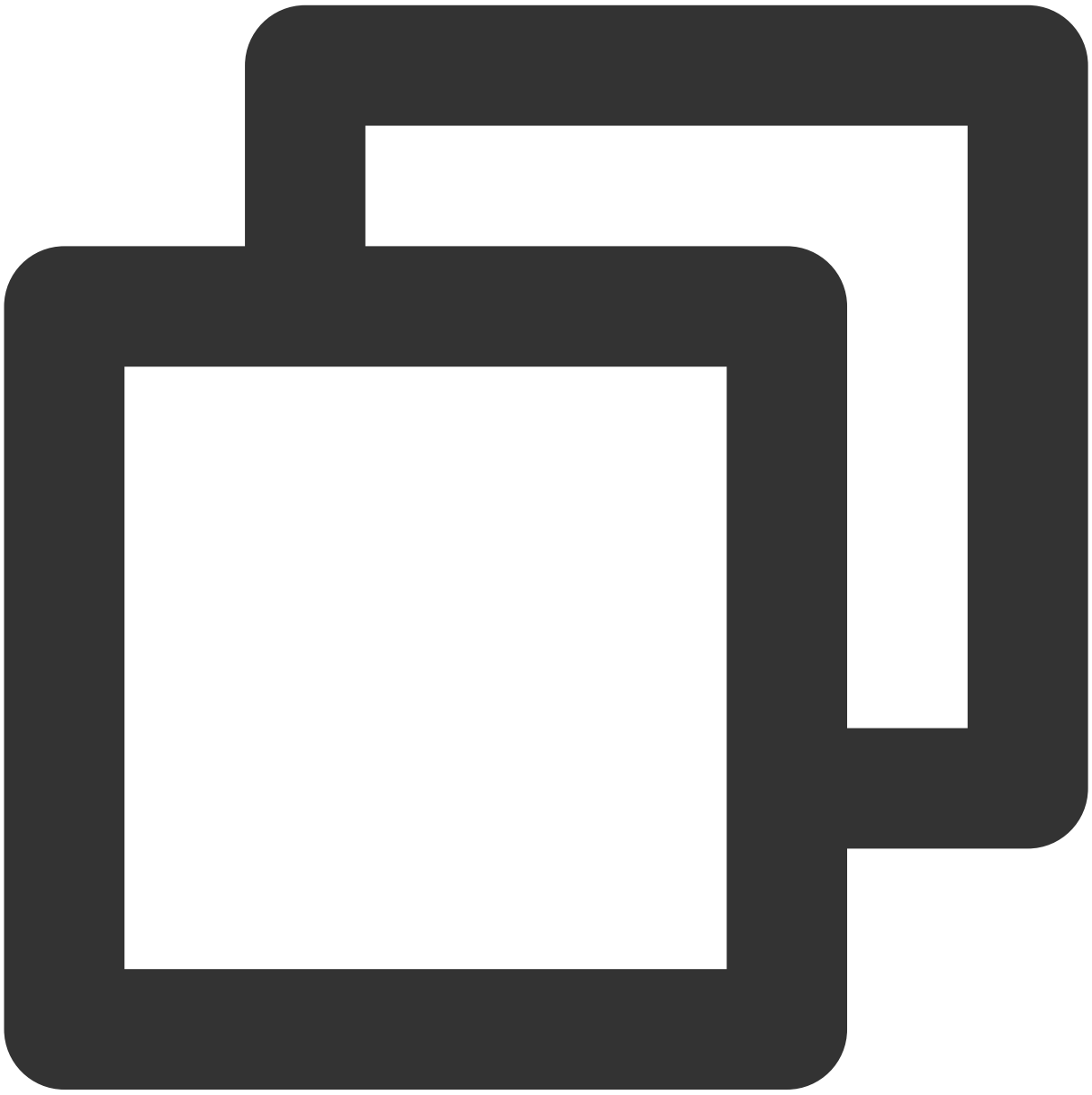
Anda harus sudah memiliki akun admin dan kata sandi (atau kunci) untuk login ke instans.
Jika Anda menggunakan kata sandi default sistem untuk masuk ke instans, buka Pusat Pesan untuk mendapatkan kata sandi terlebih dahulu.
Jika Anda menggunakan kunci untuk login, Anda harus membuat kunci dan mengikatnya ke CVM ini. Untuk informasi selengkapnya, lihat Mengelola Kunci SSH.
Jika lupa kata sandi Anda, harap atur ulang kata sandi instans Anda.
IP publik telah dibeli untuk instans CVM Anda, dan port 22 terbuka (ini terbuka secara default untuk CVM yang dibeli dengan konfigurasi cepat).

## Petunjuk

### Menggunakan kata sandi

1. Jalankan perintah berikut untuk terhubung ke CVM Linux.
**Keterangan:**

Jika komputer lokal Anda menggunakan Mac OS, Anda harus membuka terminal yang disediakan oleh sistem, lalu menjalankan perintah berikut.
Jika komputer lokal Anda menggunakan Linux, Anda dapat langsung menjalankan perintah berikut.
Jika komputer lokal Anda menggunakan Windows 10 atau Windows Server 2019, Anda harus terlebih dahulu membuka command prompt CMD, lalu menjalankan perintah berikut.



```
ssh <username>@<hostname or IP address>
```

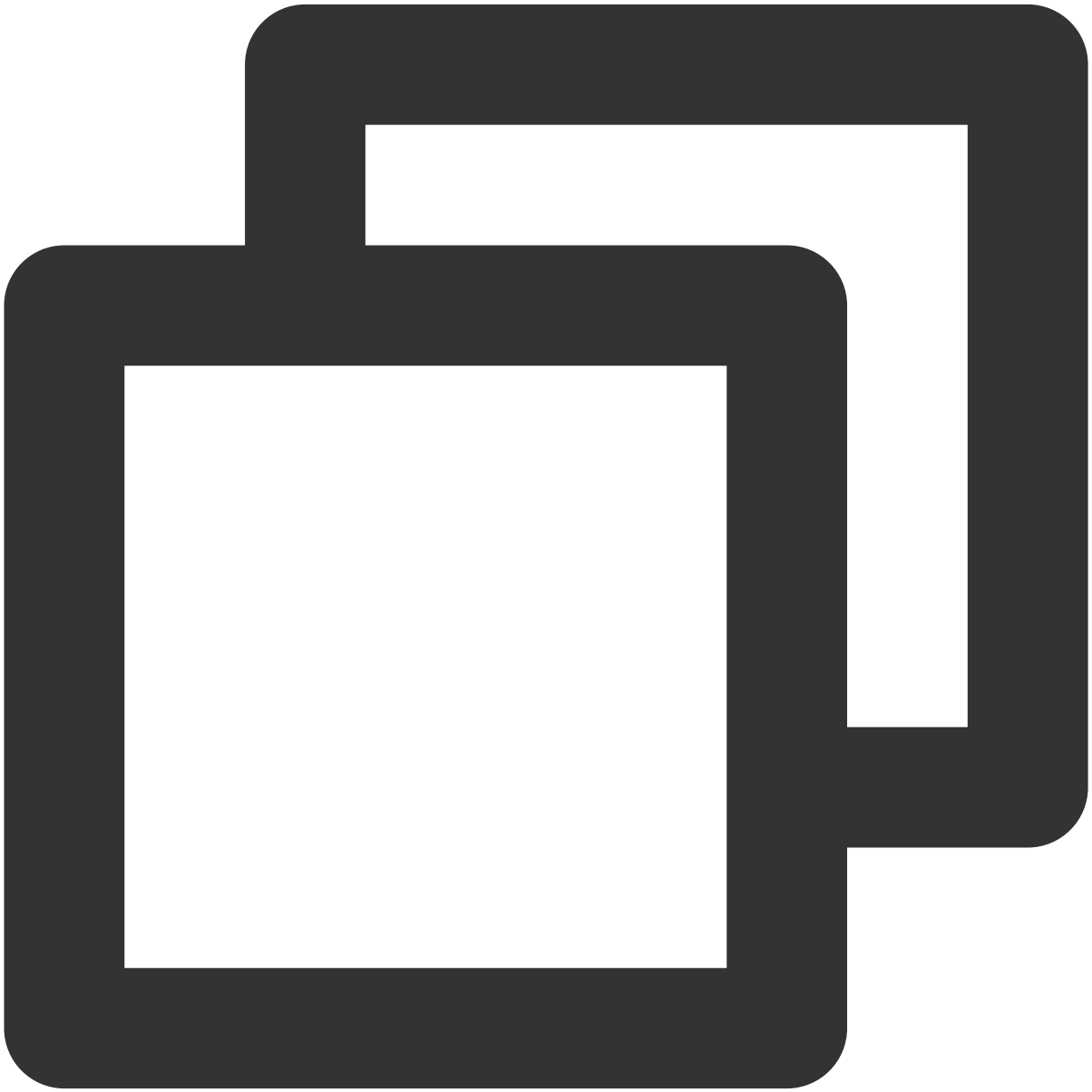
`username` mengacu pada nama akun default yang diperoleh sebagai prasyarat.

`hostname or IP address` mengacu pada alamat IP publik atau nama domain kustom dari instans Linux Anda.

2. Masukkan kata sandi yang sudah Anda peroleh, lalu tekan **Enter** (Enter) untuk login.

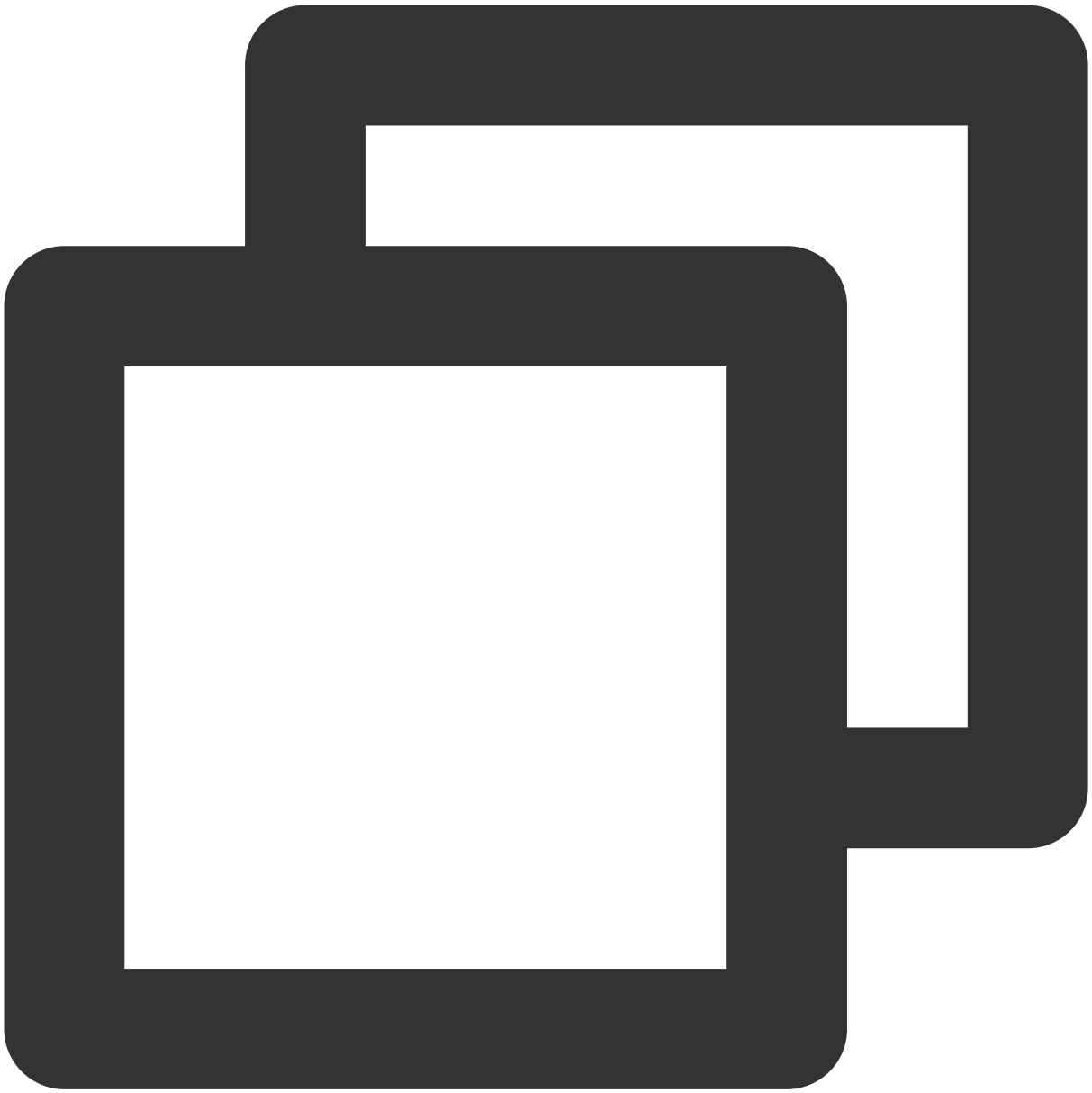
### Menggunakan kunci

1. Jalankan perintah berikut untuk mengatur file kunci pribadi yang hanya dapat dibaca oleh Anda.
Jika komputer lokal menggunakan Mac OS, Anda harus terlebih dahulu membuka terminal yang disediakan oleh sistem, lalu menjalankan perintah berikut.
Jika komputer lokal Anda menggunakan Linux, Anda dapat langsung menjalankan perintah berikut.

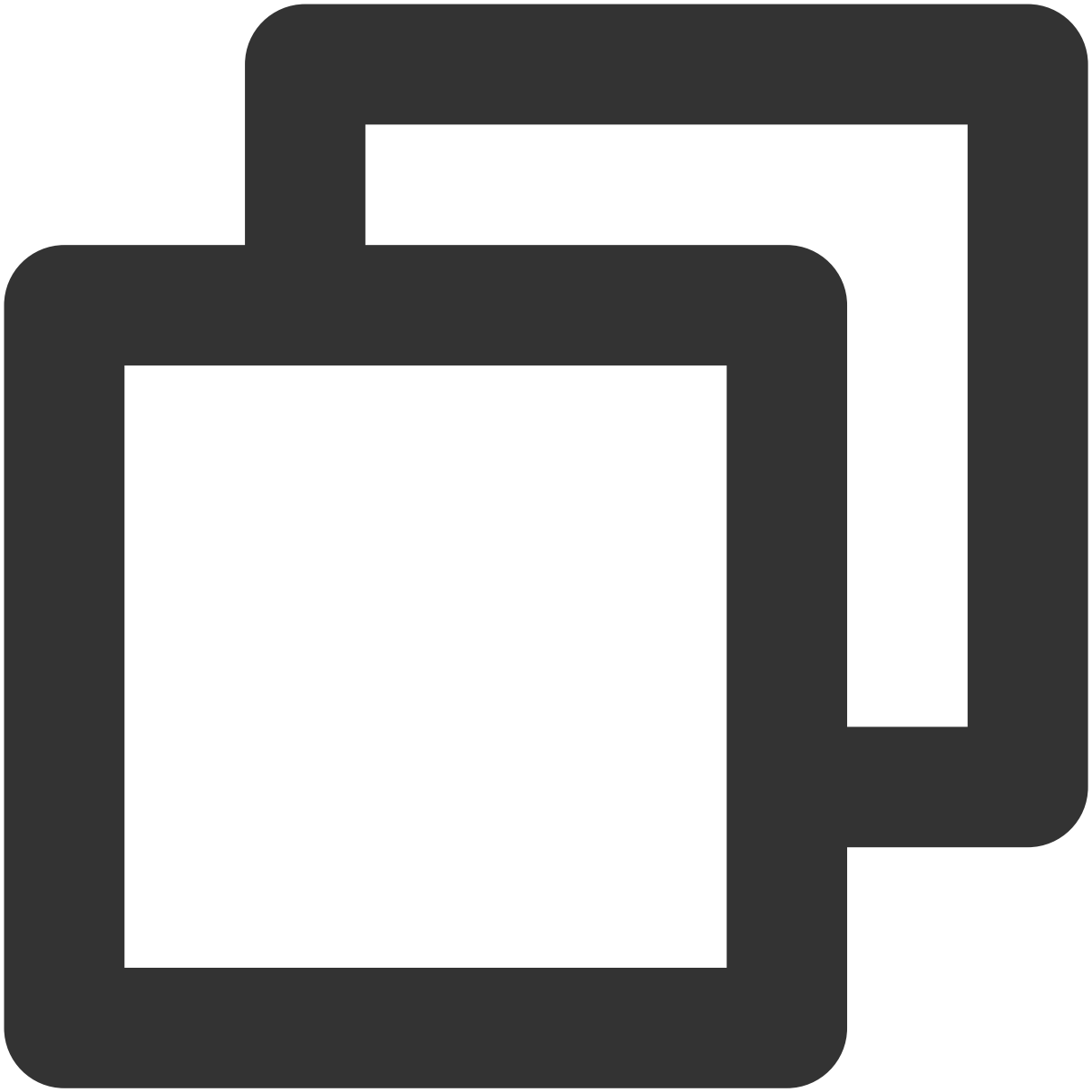


```
chmod 400 <The absolute path of the private key downloaded to be associated with th
```

Jika komputer lokal Anda menggunakan Windows 10, Anda harus terlebih dahulu membuka command prompt CMD, lalu menjalankan perintah berikut.

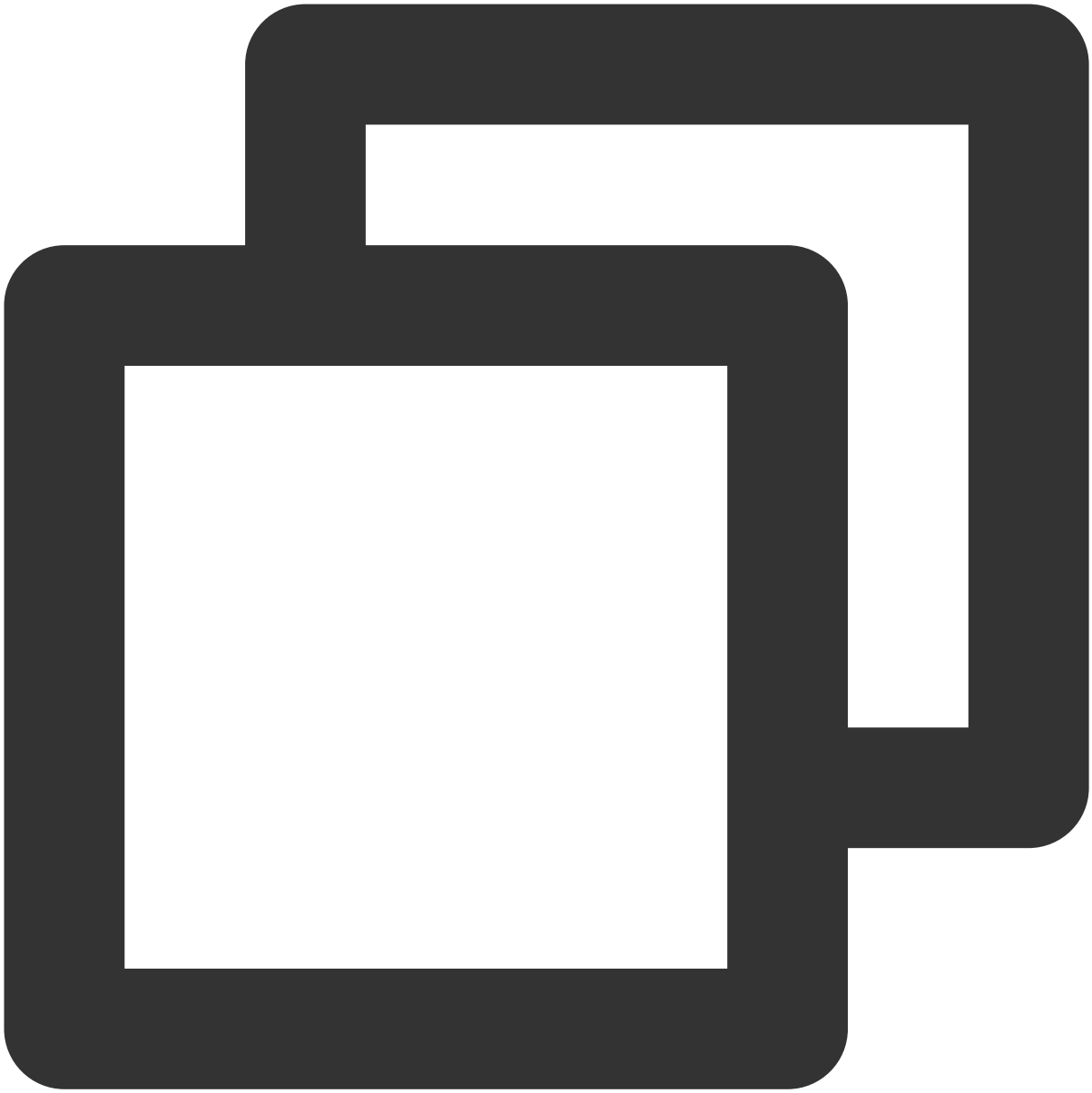


```
icacls <The absolute path of the private key downloaded to be associated with the C
```



```
icacls <The absolute path of the private key downloaded to be associated with the C
```

2. Jalankan perintah berikut untuk login jarak jauh.



```
ssh -i <The absolute path of the private key downloaded to be associated with the C
```

`username` mengacu pada nama akun default yang diperoleh sebagai prasyarat.

`hostname or IP address` mengacu pada alamat IP publik atau nama domain kustom dari instans Linux Anda. Misalnya, jalankan perintah `ssh -i "Mac/Downloads/shawn_qcloud_stable.pem" ubuntu@192.168.11.123` untuk login ke CVM Linux dari jarak jauh.

## Operasi Selanjutnya

Setelah login ke CVM, Anda dapat membangun situs web atau forum pribadi atau melakukan operasi lain. Untuk informasi selengkapnya, lihat: Membuat Situs Web WordPress Secara Manual

# Login ke Instans Linux melalui VNC

Waktu update terbaru：2021-12-13 17:07:06

## Skenario

Login VNC yang disediakan oleh Tencent Cloud memungkinkan pengguna login dari jarak jauh ke CVM melalui browser web. Jika klien tidak menginstal login jarak jauh atau tidak dapat digunakan, pengguna dapat login ke CVM menggunakan login VNC untuk memeriksa status CVM dan melakukan operasi manajemen dasar menggunakan akun CVM.

## OS yang Berlaku

Windows, Linux, atau macOS.

## Batasan Penggunaan

Login VNC saat ini tidak mendukung salin dan tempel, metode input bahasa Mandarin, serta pengunggahan atau pengunduhan file.
Saat Anda menggunakan VNC untuk login ke CVM, browser utama harus digunakan, seperti Chrome, Firefox, IE 10, dan versi yang lebih baru.
Login VNC adalah terminal khusus, artinya hanya satu pengguna yang dapat menggunakan login VNC pada satu waktu.

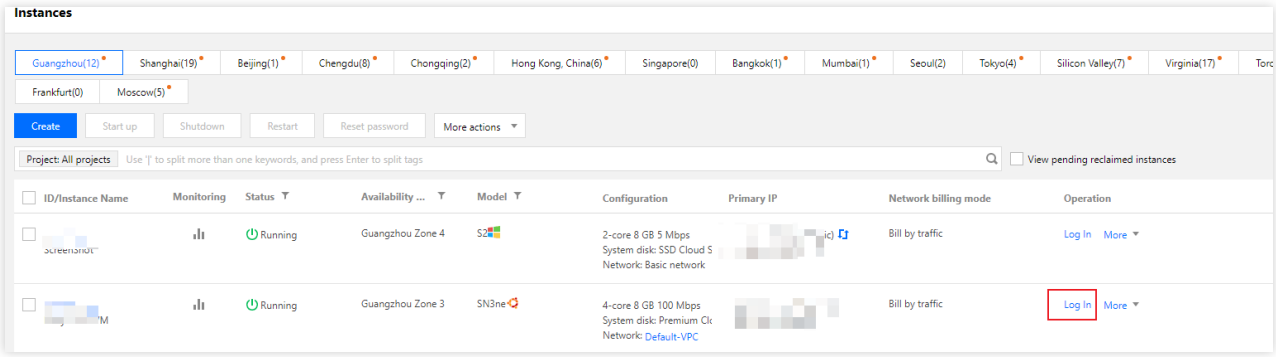
## Prasyarat

Anda harus sudah memiliki akun admin dan kata sandi instans Linux tempat Anda login.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, pertama-tama buka Pesan Internal untuk mendapatkannya.
Jika Anda lupa kata sandi Anda, harap atur ulang kata sandi instans.

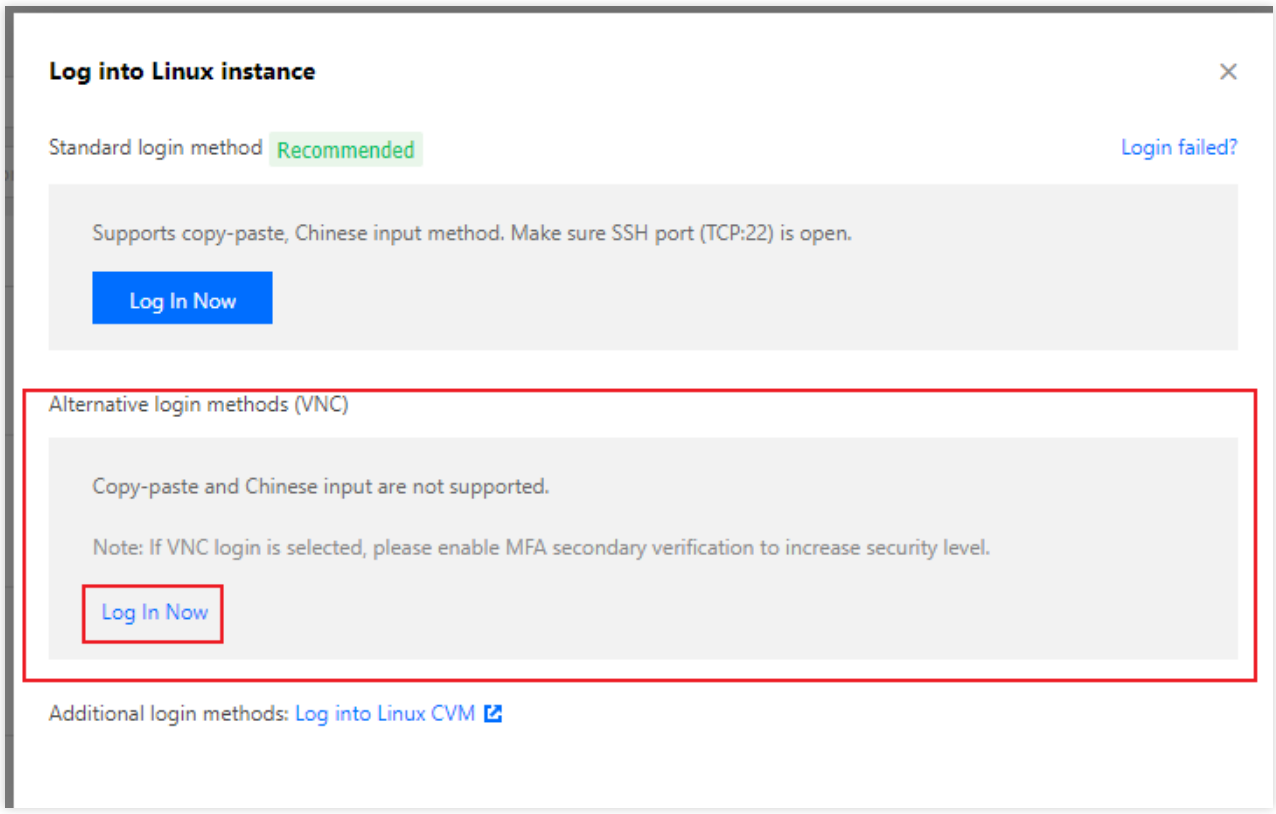
## Petunjuk

1. Login ke Konsol CVM.

2. Pada halaman manajemen Instans, pilih CVM Linux tempat Anda ingin login dan klik **Log In** (Login), seperti yang ditunjukkan di bawah ini:



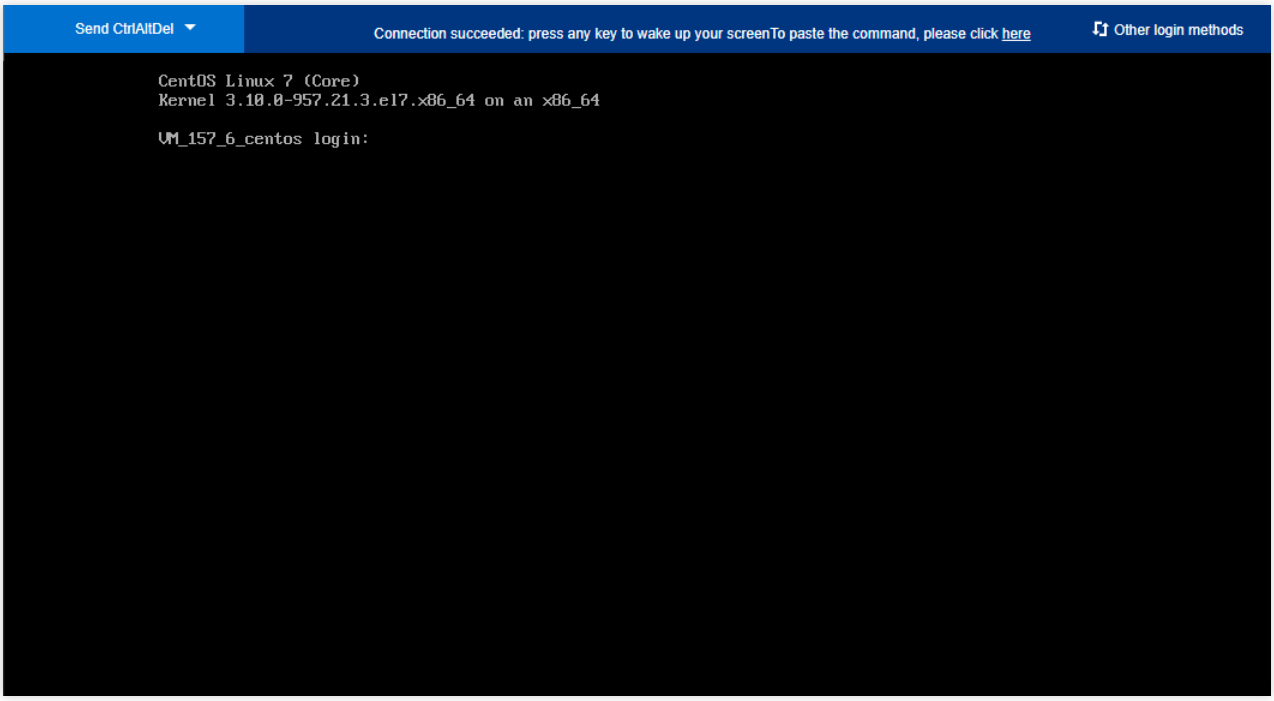

3. Di jendela **Log into Linux instance** (Login ke instans Linux) yang muncul, pilih **Alternative login methods (VNC)** (Metode login alternatif (VNC)), lalu klik **Log In Now** (Login Sekarang), seperti yang ditunjukkan di bawah ini.




4. Di kotak dialog pop-up, masukkan nama pengguna setelah **login** (login), lalu tekan **Enter** (Enter).

5. Masukkan kata sandi setelah **Password** (Kata Sandi), lalu tekan **Enter** (Enter).

Kata sandi yang dimasukkan tidak ditampilkan secara default, seperti yang ditunjukkan di bawah ini:




Setelah login, informasi tentang CVM tempat Anda login saat ini muncul di sebelah kiri command prompt.

## Operasi Selanjutnya

Setelah login ke CVM, Anda dapat membangun situs web atau forum pribadi atau melakukan operasi lain. Untuk informasi selengkapnya, lihat dokumen berikut:

Operasi dan Perintah Umum

Membuat situs WordPress pribadi

Membuat forum Diskuz!

# Login ke Instans Linux dari Perangkat Seluler

Waktu update terbaru：2021-12-13 17:07:06

## Ikhtisar

Dokumen ini menjelaskan cara login ke instans Linux dari perangkat seluler yang berbeda. Alat berikut digunakan sebagai contoh.
Perangkat iOS: Klien Termius-SSH
Perangkat Android: JuiceSSH

## Perangkat Seluler yang Berlaku

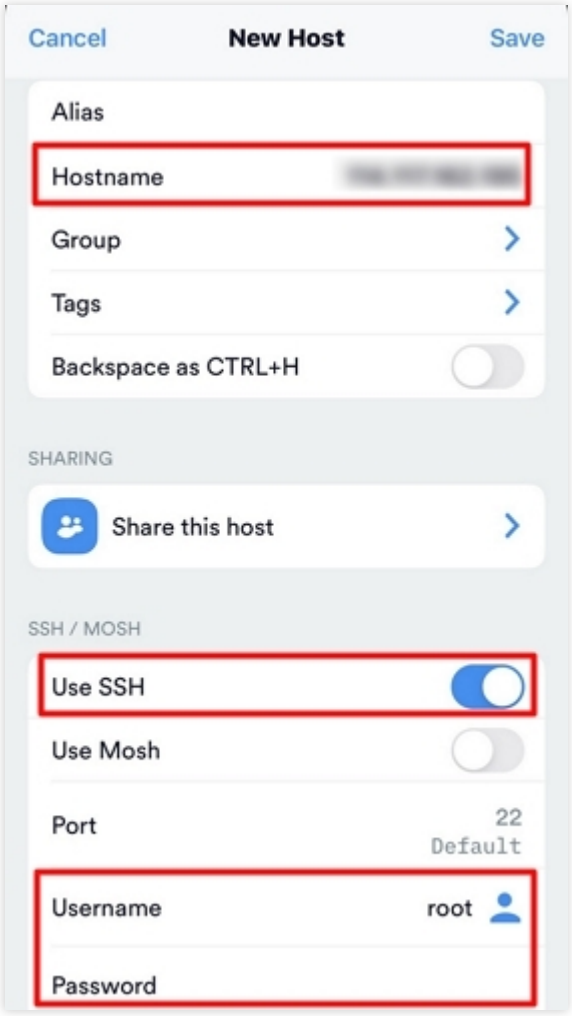
Perangkat iOS dan Android

## Prasyarat

Instans CVM dalam status **Running** (Berjalan).
Anda sudah memiliki akun admin dan kata sandi (atau kunci) untuk digunakan login ke instans.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, buka Pusat Pesan untuk mendapatkan kata sandi terlebih dahulu.
Jika lupa kata sandi, Anda dapat atur ulang sandi instans.
IP publik telah dibeli untuk instans CVM Anda, dan port 22 terbuka. Port ini terbuka secara default untuk instans CVM yang dibeli dengan konfigurasi cepat.

## Petunjuk

Login ke instans dari perangkat seluler yang Anda gunakan:
iOS device
Android device
1. Unduh klien Termius-SSH dari App Store, dan daftar seperti yang diinstruksikan.
2. Ketuk **New Host** (Host Baru) di layar beranda.
3. Akses halaman **New Host** (Host Baru) dan konfigurasikan informasi login sebagai berikut:




**Hostname** (Nama host): alamat IP publik instans CVM Anda. Untuk informasi selengkapnya, lihat Mendapatkan Alamat IP Publik.

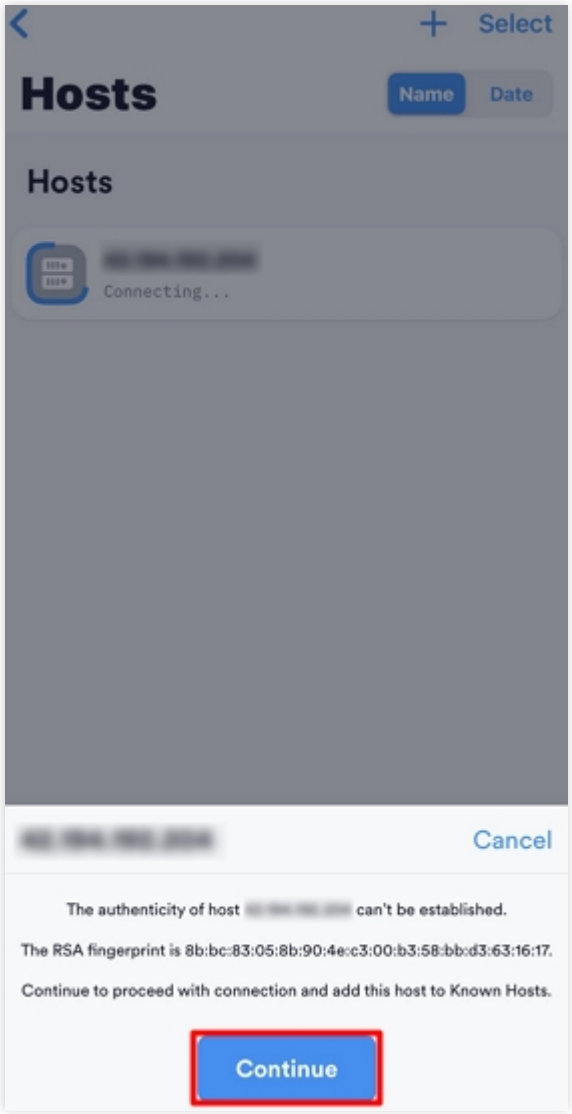
**Use SSH** (Gunakan SSH): diaktifkan secara default.

**Username** (Nama Pengguna): masukkan akun admin `root`, atau `ubuntu` jika instans Anda menggunakan sistem operasi Ubuntu.

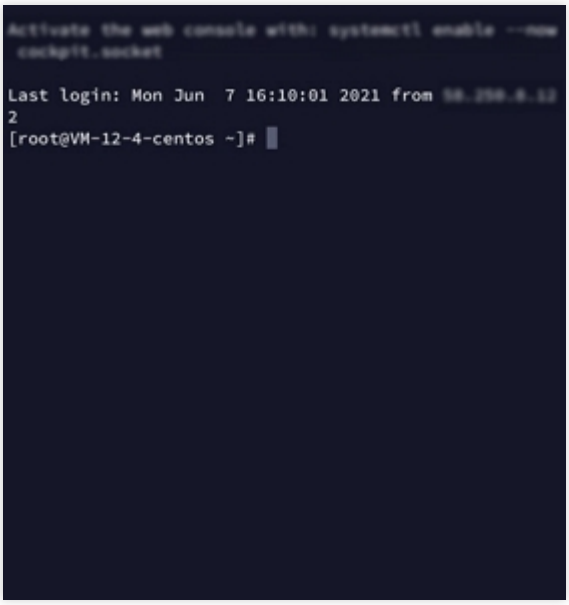
**Password** (Kata Sandi): masukkan kata sandi login instans.

4. Ketuk **Save** (Simpan) di sudut kanan atas untuk menyimpan konfigurasi login.

5. Pilih informasi login di halaman **Hosts** (Host), lalu ketuk **Continue** (Lanjutkan) di kotak prompt di bagian bawah halaman.




6. Login berhasil jika Anda melihat hal berikut.




**Membuat identitas**

1. Unduh dan instal JuiceSSH.
2. Dari layar beranda, ketuk **Connections** (Koneksi) untuk membuka tab **Identity** (Identitas).
3. Ketuk **+** (+) di sudut kanan bawah.
4. Konfigurasikan nama akun dan kata sandi di halaman **Identity** (Identitas).

**Nickname** (Nama panggilan): masukkan nama kustom untuk identitas, hal ini bersifat opsional.

**Username** (Nama Pengguna): masukkan akun admin `root` , atau `ubuntu` jika instans Anda menggunakan sistem operasi Ubuntu.

**Password** (Kata Sandi): ketuk **Set (optional)** (Atur (opsional)), lalu masukkan kata sandi login instans di jendela pop-up.

5. Ketuk ✔ (✔) di sudut kanan atas halaman.

**Membuat koneksi**

1. Dari layar beranda, ketuk **Connection** (Koneksi), lalu ketuk **+** (+) di sudut kanan bawah halaman **Connections** (Koneksi).
2. Konfigurasikan informasi login untuk koneksi baru.

**Nickname** (Nama Panggilan): masukkan nama koneksi khusus, hal ini bersifat opsional.

**Type** (Jenis): pilih **SSH** (SSH).

**Address** (Alamat): alamat IP publik instans CVM Anda. Untuk informasi selengkapnya, lihat Mendapatkan Alamat IP Publik.

**Identity** (Identitas): pilih identitas yang dibuat di Membuat identitas.

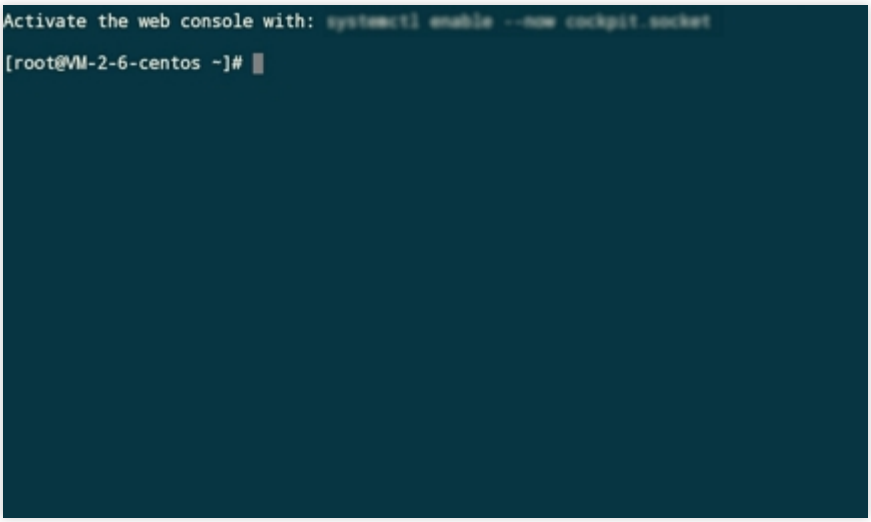
**Port** (Port): masukkan port 22.

Pertahankan pengaturan default untuk parameter lainnya.

3. Ketuk **Add to team** (Tambahkan ke tim) di bagian bawah halaman untuk menyimpan konfigurasi login.

### Login ke instans

1. Pada halaman **Connections** (Koneksi), pilih instans untuk login dan ketuk **Accept** (Terima).
2. Login berhasil jika Anda melihat hal berikut.



# Login ke instans Windows
# Login ke Instans Windows Menggunakan RDP

Waktu update terbaru：2022-01-07 10:19:20

## Ikhtisar

Remote Desktop Protocol (RDP) adalah protokol multi-saluran yang dikembangkan oleh Microsoft yang memungkinkan komputer lokal terhubung ke komputer jarak jauh. Sebaiknya gunakan RDP untuk login ke CVM Windows Anda. Dokumen ini menjelaskan cara login ke instans Windows menggunakan file RDP.

## Sistem yang Didukung

Anda dapat login ke CVM Anda dari Windows, Linux, dan MacOS menggunakan RDP.

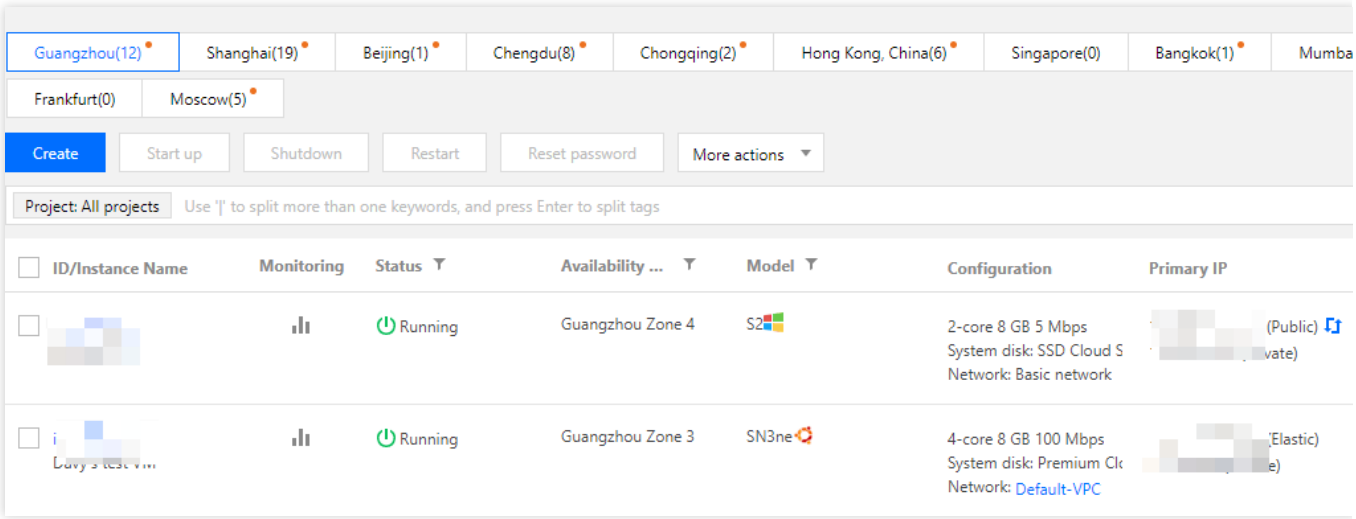
## Prasyarat

Anda harus memiliki akun admin dan kata sandi untuk login ke instans Windows dari jarak jauh.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, Anda dapat memperoleh kata sandi di Pusat Pesan.
Jika Anda lupa kata sandi, harap atur ulang kata sandi instans.
Anda telah membeli IP publik untuk instans CVM Anda dan port 3389 terbuka. (port ini terbuka secara default untuk CVM yang dibeli dengan konfigurasi cepat).

## Petunjuk

### Login ke CVM Anda di Windows menggunakan RDP

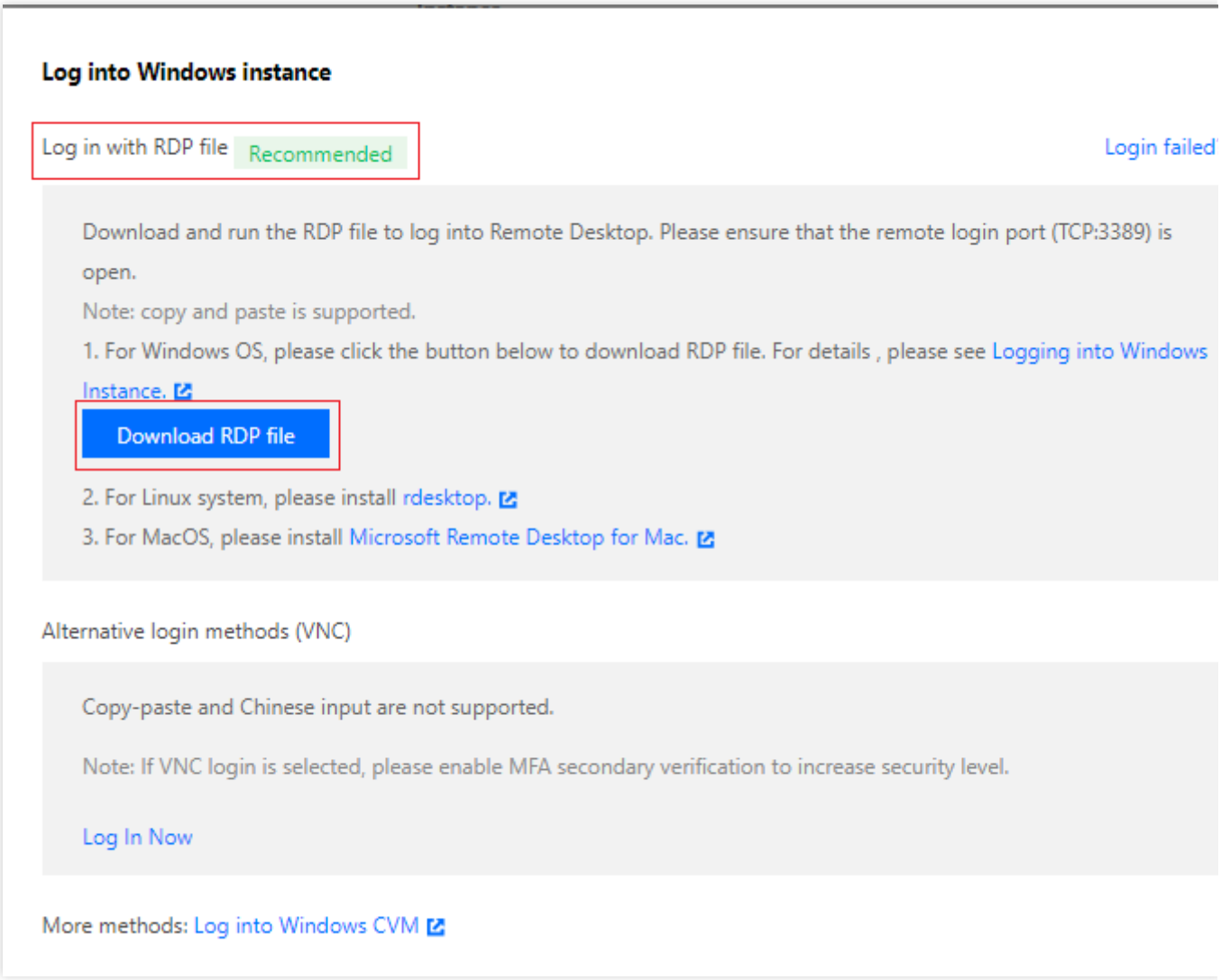
1. Login ke Konsol CVM.
2. Pada halaman **Instances** (Instans), cari CVM Windows tempat Anda ingin login, lalu klik **Log In** (Login) seperti yang ditunjukkan di bawah ini.




3. Di jendela pop-up **Log into Windows instance** (Login ke instans Windows), pilih **Log in with RDP file** (Login dengan file RDP) dan klik **Download RDP file** (Unduh file RDP) untuk mengunggah file RDP ke komputer lokal Anda.

**Keterangan:**

Jika Anda telah mengubah port login jarak jauh, tambahkan alamat IP dengan `:port` di file RDP.




4. Klik dua kali file RDP yang diunduh, masukkan kata sandi, lalu klik **OK** (OKE) untuk menyambungkan ke CVM Windows Anda dari jarak jauh.

Jika Anda menggunakan kata sandi default sistem untuk login ke instans, Anda dapat memperoleh kata sandi di Pusat Pesan.

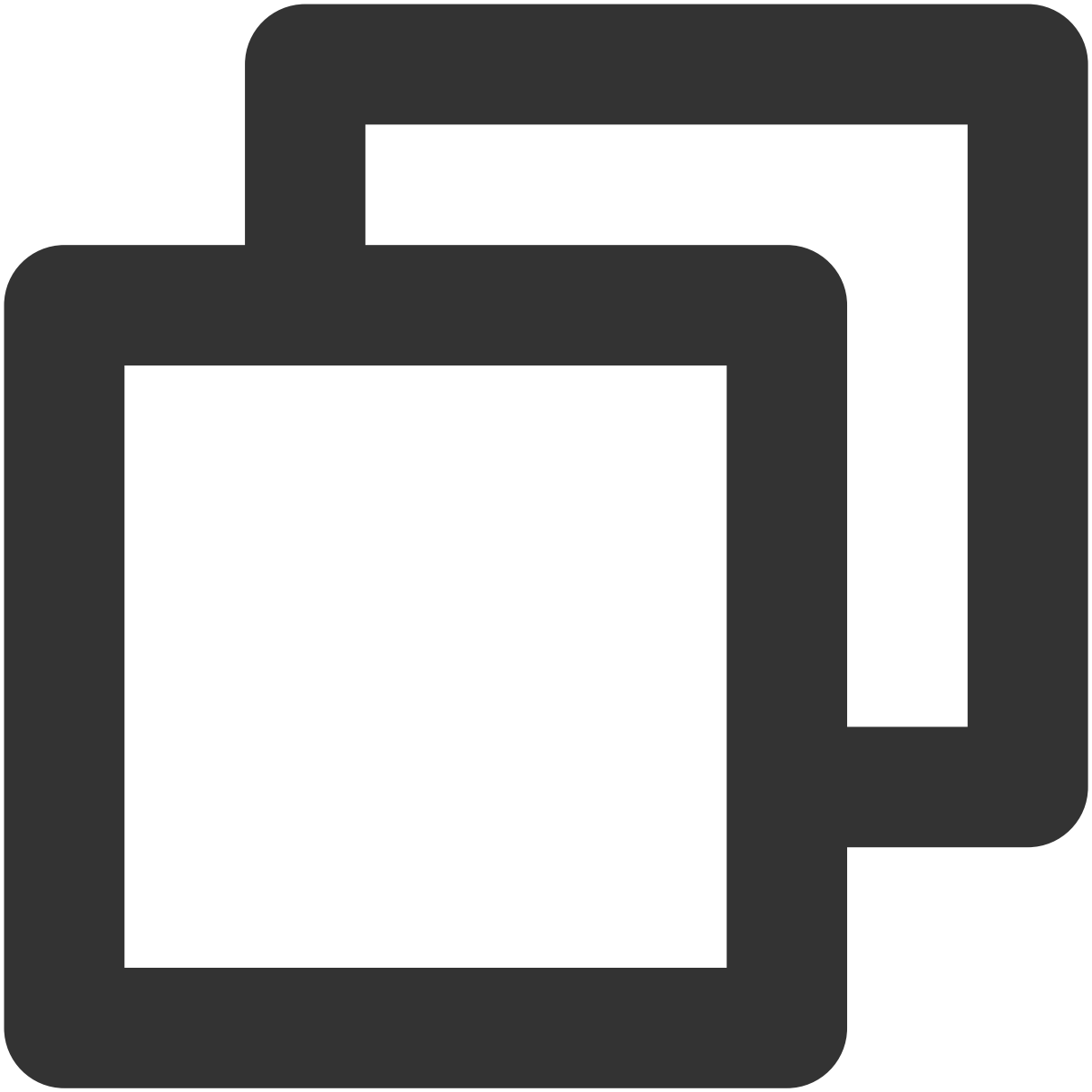
Jika Anda lupa kata sandi, harap atur ulang kata sandi instans.

## Login ke CVM Anda di Linux menggunakan RDP

**Keterangan:**

Sebaiknya gunakan rdesktop sebagai klien desktop jarak jauh. Untuk informasi selengkapnya, lihat pengantar resmi rdesktop.

1. Jalankan perintah berikut untuk memeriksa apakah rdesktop telah diinstal.



```
rdesktop
```

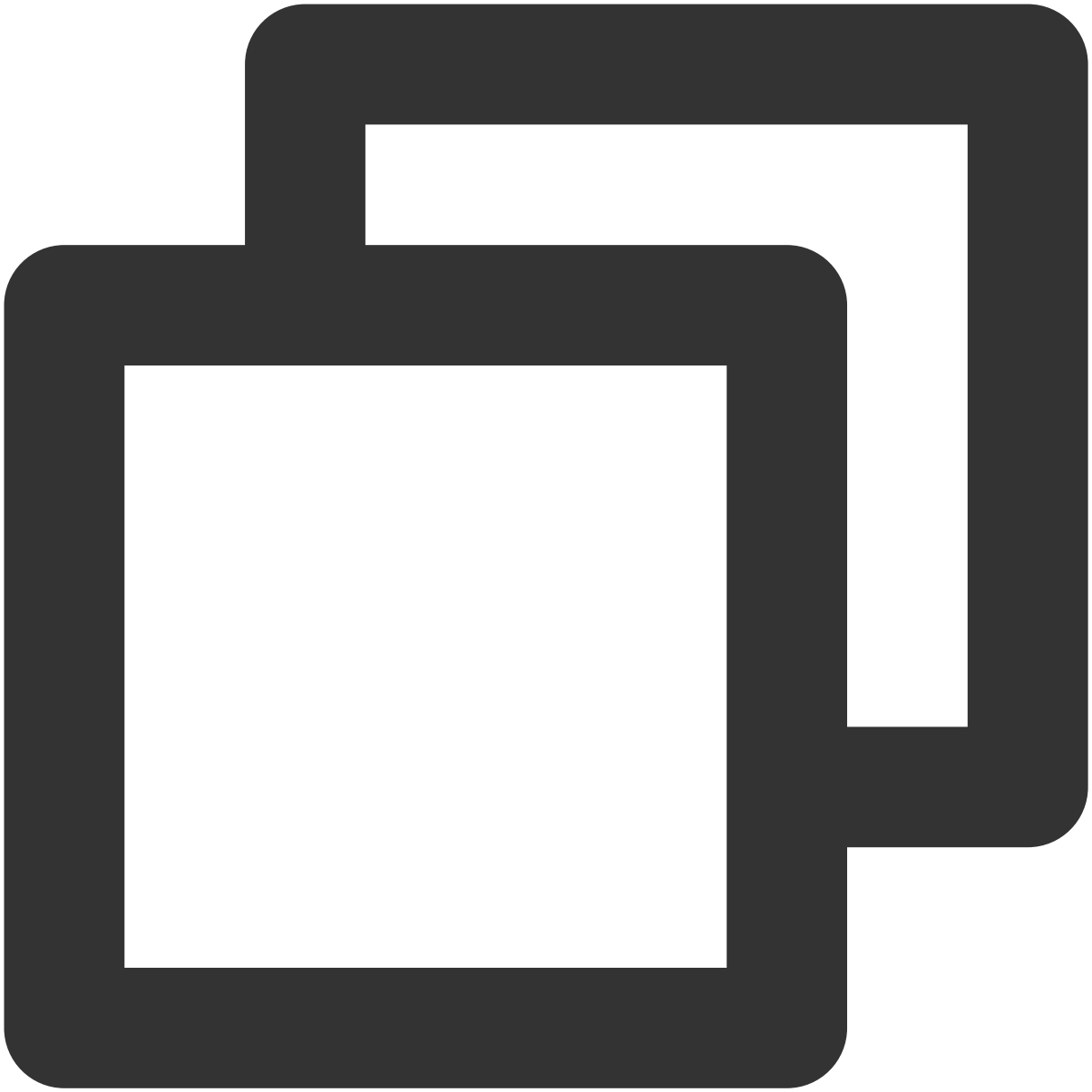
Jika ya, lakukan langkah 4.

Jika tidak, Anda akan diminta dengan "command not found" (perintah tidak ditemukan). Dalam hal ini, lakukan langkah 2.

2.

Buka jendela terminal

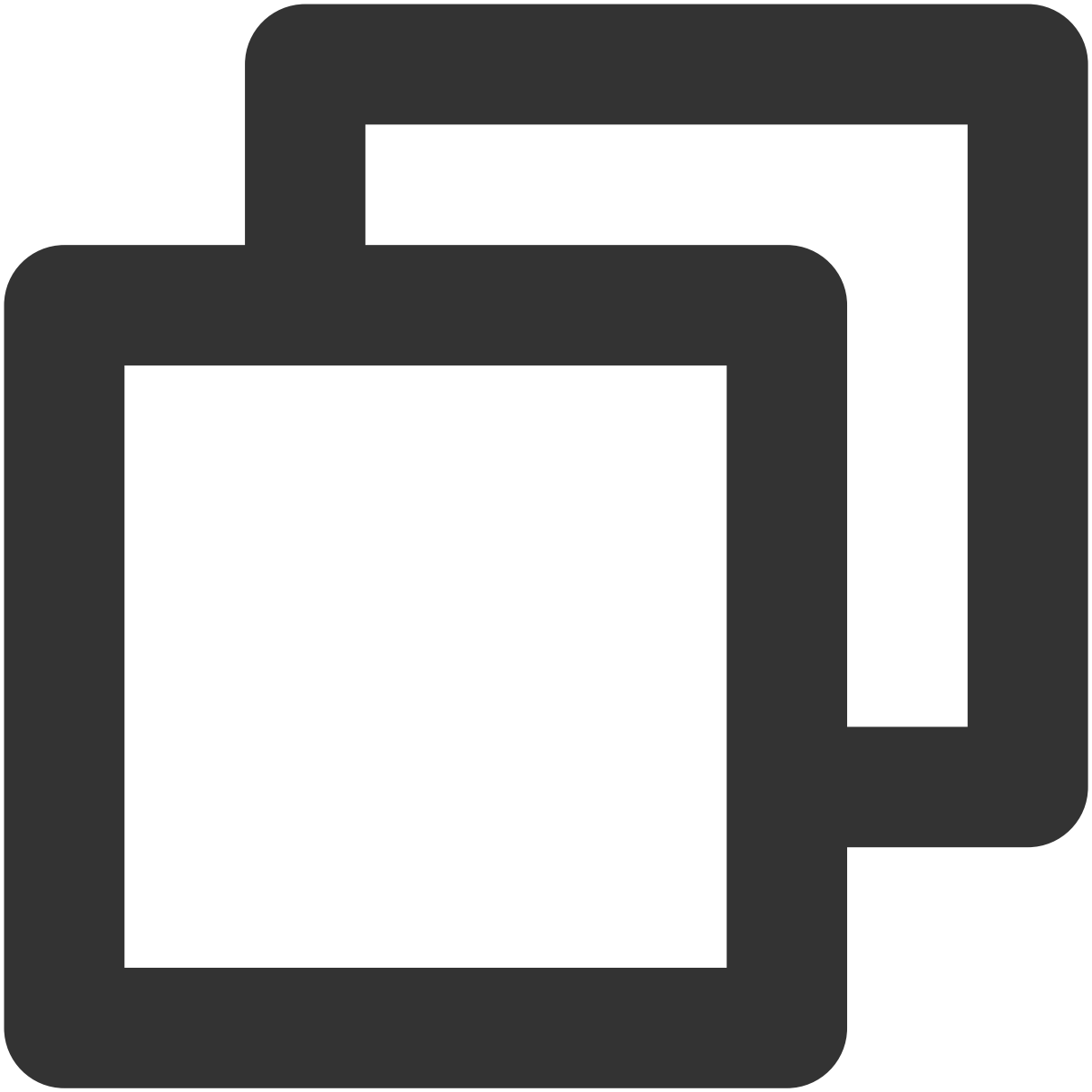
, lalu jalankan perintah berikut untuk mengunduh rdesktop. Langkah ini menggunakan rdesktop v1.8.3 sebagai contoh.



```
wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.t
```

Jika Anda ingin menginstal versi terbaru, buka halaman desktop di GitHub untuk menemukannya. Kemudian, ganti jalur dalam perintah dengan versi terbaru.

3. Di direktori tempat rdesktop akan diinstal, jalankan perintah berikut untuk mendekompresi dan menginstal rdesktop.



```
tar xvzf rdesktop-<x.x.x>.tar.gz ## Ganti x.x.x dengan nomor versi rdesktop yang di
cd rdesktop-1.8.3
./configure
make
make install
```

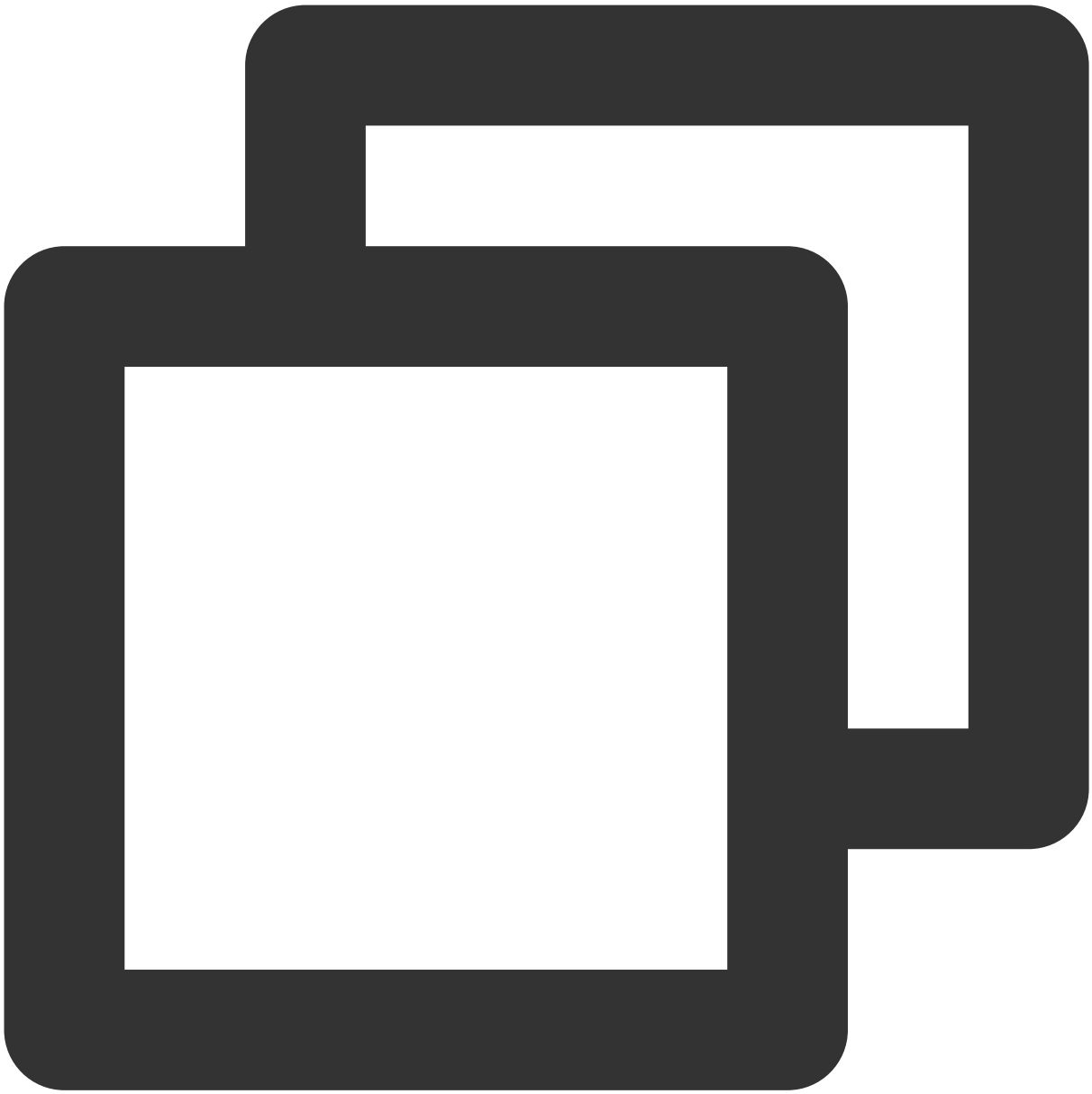
4.

Jalankan perintah berikut

untuk terhubung ke instans Windows jarak jauh.

**Keterangan:**

Ganti parameter dalam contoh dengan parameter Anda sendiri.



```
rdesktop -u Administrator -p <your-password> <hostname or IP address>
```

`Administrator` mengacu pada akun admin yang disebutkan di bagian prasyarat.

`<your-password>` mengacu pada kata sandi login yang Anda tetapkan.

Jika Anda menggunakan kata sandi default sistem untuk masuk ke instans, Anda dapat memperoleh kata sandi di Pusat Pesan. Jika Anda lupa kata sandi Anda, harap atur ulang kata sandi instans.

`<hostname or IP address>` mengacu pada alamat IP publik atau nama domain kustom dari instans Windows Anda.

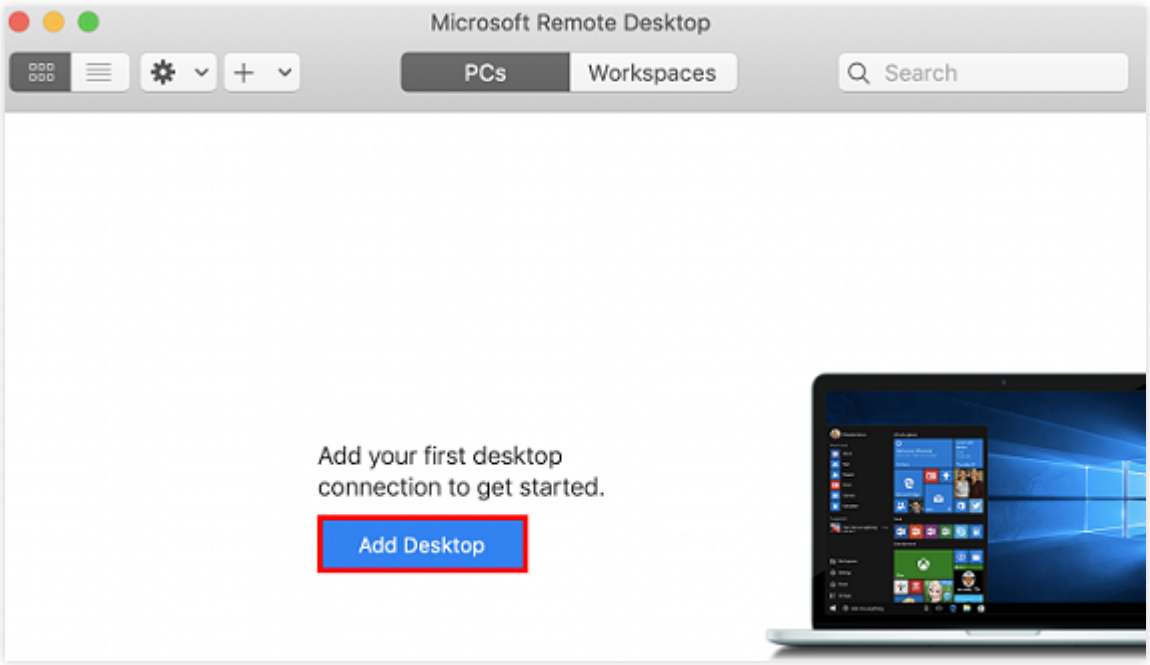
## Login ke CVM Anda di MacOS menggunakan RDP

**Keterangan:**

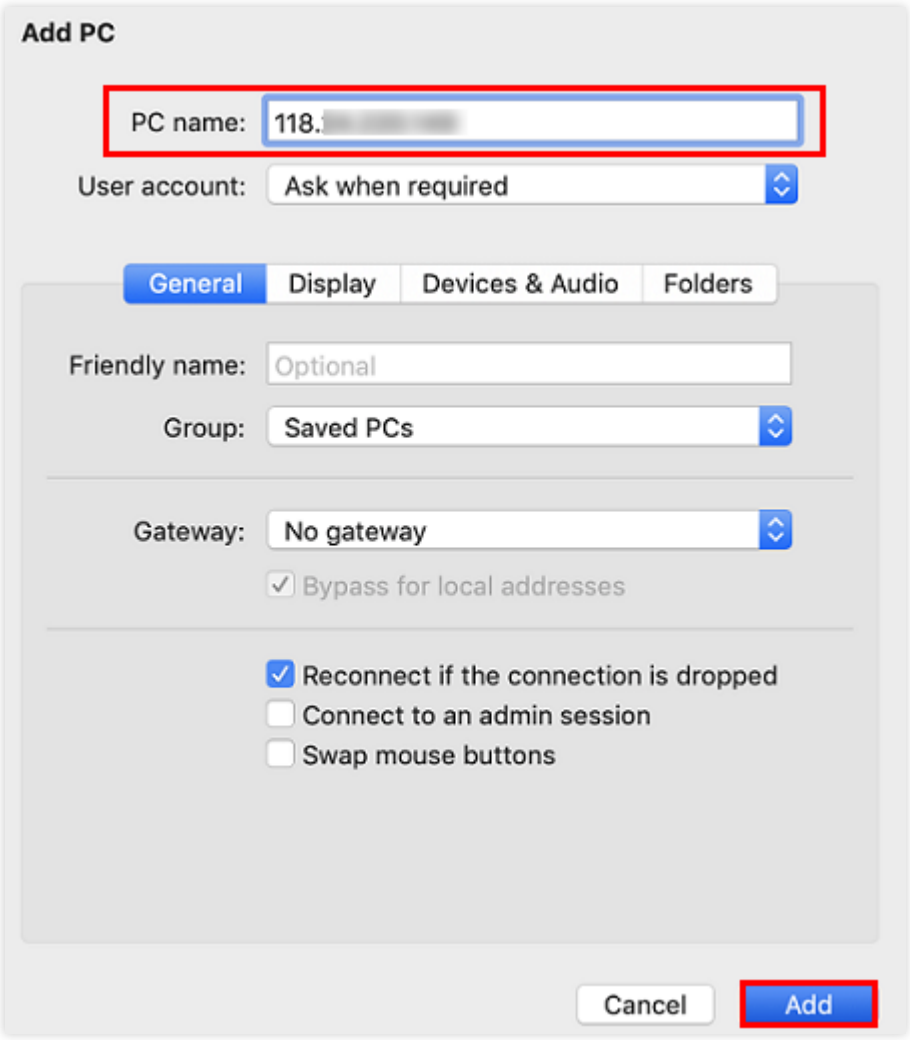
Operasi berikut menggunakan Microsoft Remote Desktop untuk Mac sebagai contoh. Microsoft berhenti menyediakan tautan untuk mengunduh klien Remote Desktop pada tahun 2017. Saat ini, anak perusahaannya, HockeyApp, bertanggung jawab untuk merilis klien beta. Buka Microsoft Remote Desktop Beta untuk mengunduh versi Beta.

Operasi berikut menggunakan CVM pada Windows Server 2012 R2 sebagai contoh.

1. Unduh dan instal Microsoft Remote Desktop untuk Mac di komputer lokal Anda.
2. Mulai MRD dan klik **Add Desktop** (Tambahkan Desktop), seperti yang ditunjukkan di bawah ini:




3. Di jendela pop-up **Add Desktop** (Tambahkan Desktop), ikuti langkah-langkah yang diilustrasikan pada citra berikut untuk membuat koneksi ke CVM Windows Anda.

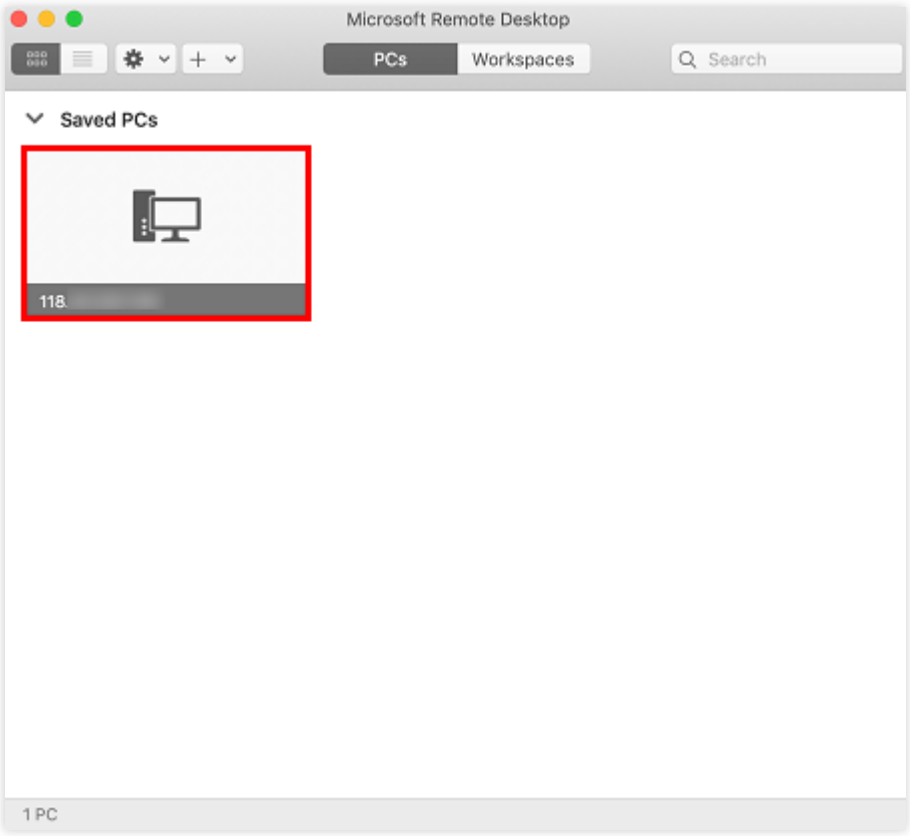



3.1 Di kolom teks **PC name** (Nama PC), masukkan alamat IP publik CVM Anda.

3.2 Klik **Add** (Tambahkan).

3.3 Pertahankan pengaturan default untuk opsi lain, lalu buat koneksi.

Entri Anda sekarang telah disimpan, seperti yang ditunjukkan di bawah ini:

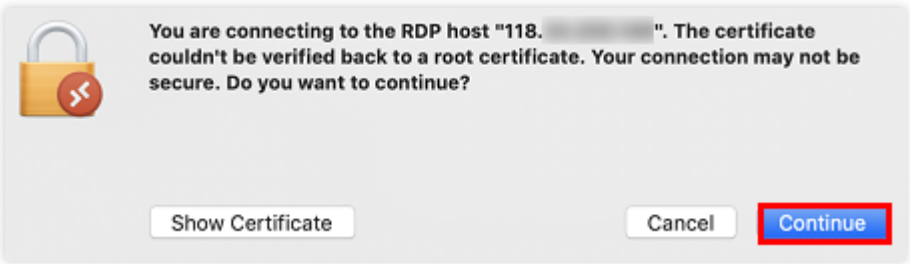



4. Klik dua kali entri baru. Masukkan nama pengguna dan kata sandi Anda untuk CVM, lalu klik **Continue** (Lanjutkan).

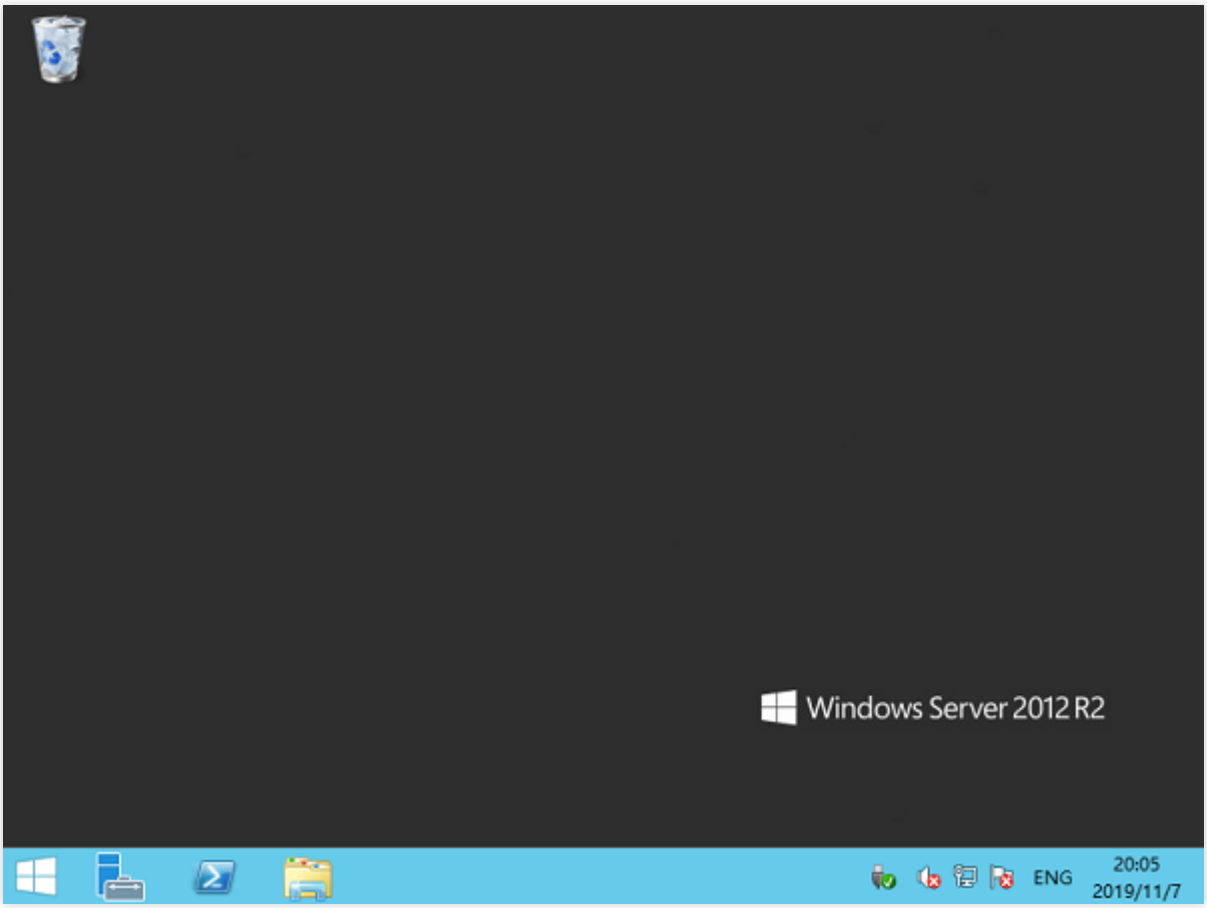
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, Anda dapat memperoleh kata sandi di Pusat Pesan.

Jika Anda lupa kata sandi, harap atur ulang kata sandi instans.

5. Di jendela pop-up, klik **Continue** (Lanjutkan) untuk membuat koneksi, seperti yang ditunjukkan di bawah ini:




Jika koneksi berhasil, akan muncul halaman berikut:



# Login ke Instans Windows melalui Desktop Jarak Jauh

Waktu update terbaru：2021-12-13 17:07:07

## Skenario

Dokumen ini menjelaskan cara login ke instans Windows melalui desktop jarak jauh di komputer lokal.

## OS yang Berlaku

Windows

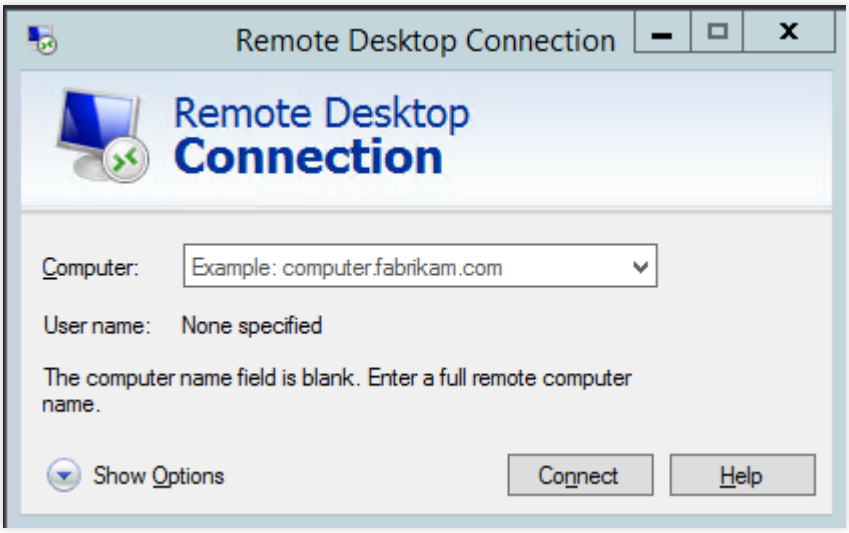
## Prasyarat

Anda harus sudah memiliki akun/kata sandi admin untuk login ke instans Windows dari jarak jauh.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, dapatkan dengan membuka Pesan Internal.
Jika Anda lupa kata sandi, atur ulang kata sandi instans.
IP publik telah dibeli untuk instans CVM Anda, dan port 3389 terbuka (jika CVM dibeli dengan “Konfigurasi Cepat”, port ini terbuka secara default.)

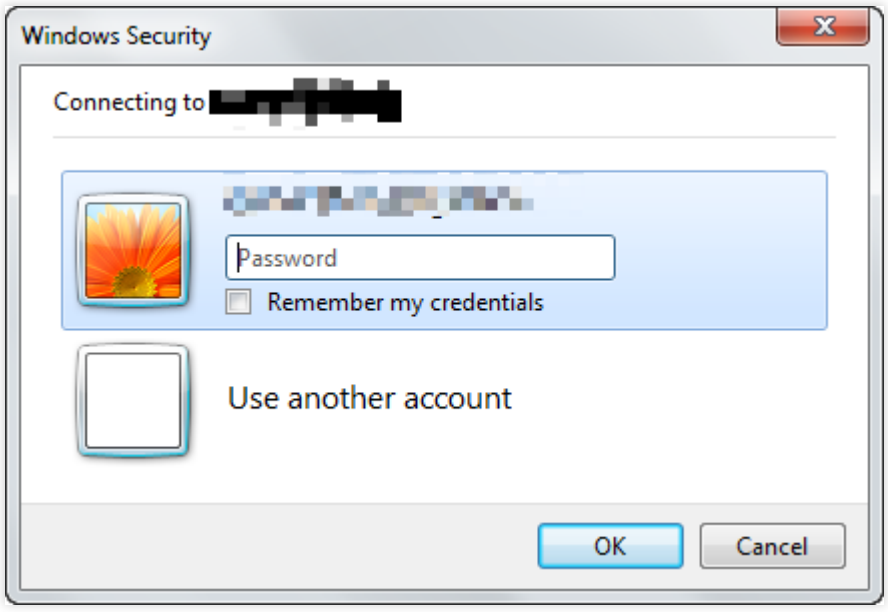
## Langkah-Langkah

**Keterangan:**
Langkah-langkah berikut mengambil sistem operasi Windows 7 sebagai contoh.
1. Di komputer Windows lokal, klik

, dan masukkan **mstsc** (mstsc) di **Search program and files** (Cari program dan file), lalu tekan **Enter** (Enter) untuk membuka kotak dialog koneksi desktop jarak jauh, seperti yang ditunjukkan di bawah ini:




2. Masukkan IP publik server Windows setelah **Computer** (Komputer), lalu klik **Connect** (Hubungkan).
Untuk informasi selengkapnya tentang cara mendapatkan IP publik, lihat Mendapatkan Alamat IP Publik.
3. Masukkan akun/kata sandi admin instans di jendela pop-up **Windows Security** (Keamanan Windows), seperti yang ditunjukkan di bawah ini:
**Keterangan:**
Jika kotak dialog **Do you trust this remote connection?** (Apakah Anda percaya koneksi jarak jauh ini?) muncul, Anda dapat mencentang **Don't ask me again for this connection to this computer** (Jangan tanya saya lagi untuk koneksi ke komputer ini), lalu klik **Connect** (Hubungkan).




4. Klik **OK** (OKE) untuk login ke instans CVM Windows.

# Login ke Instans Linux melalui VNC

Waktu update terbaru：2021-12-13 17:07:07

## Skenario

Login VNC yang ditawarkan oleh Tencent memungkinkan pengguna terhubung dari jarak jauh ke CVM melalui browser web. Jika klien tidak menginstal login jarak jauh, metode tersebut tidak dapat digunakan atau login melalui cara lain, pengguna dapat terhubung ke CVM menggunakan login VNC untuk mengamati status CVM dan melakukan operasi manajemen CVM dasar menggunakan akun CVM.

## Batasan Penggunaan

Fitur seperti salin/tempel, masukan bahasa Mandarin, dan unggah/unduh file saat ini tidak didukung pada CVM yang menggunakan login VNC.
Browser umum harus digunakan saat menggunakan login VNC pada CVM, seperti Chrome, Firefox, dan IE 10 atau yang lebih baru.
Login VNC adalah terminal khusus, artinya hanya satu pengguna yang dapat menggunakan login VNC pada satu waktu.

## OS yang Berlaku

Windows, Linux, atau macOS.

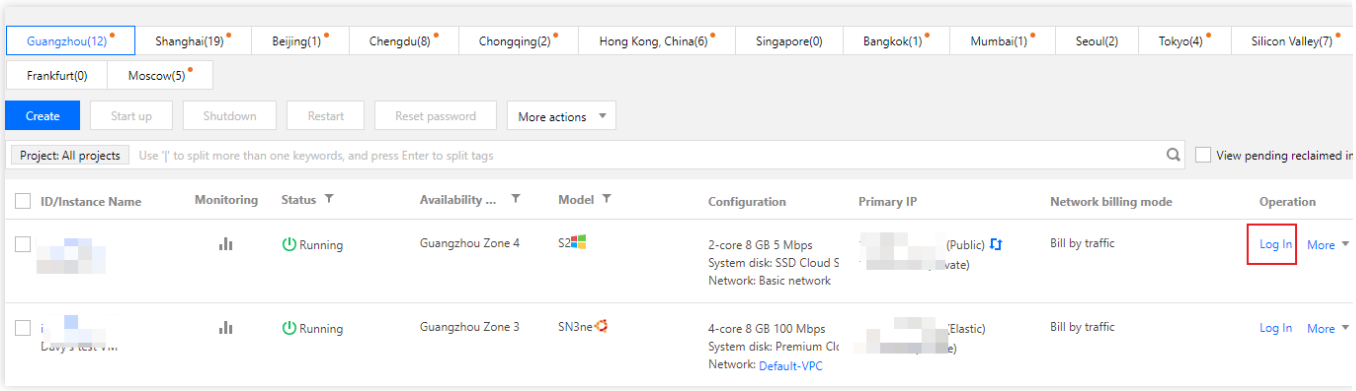
## Prasyarat

Anda harus sudah memiliki akun/kata sandi admin untuk login ke instans Windows dari jarak jauh.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, dapatkan dengan membuka Pesan Internal.
Jika Anda lupa kata sandi, atur ulang kata sandi instans.

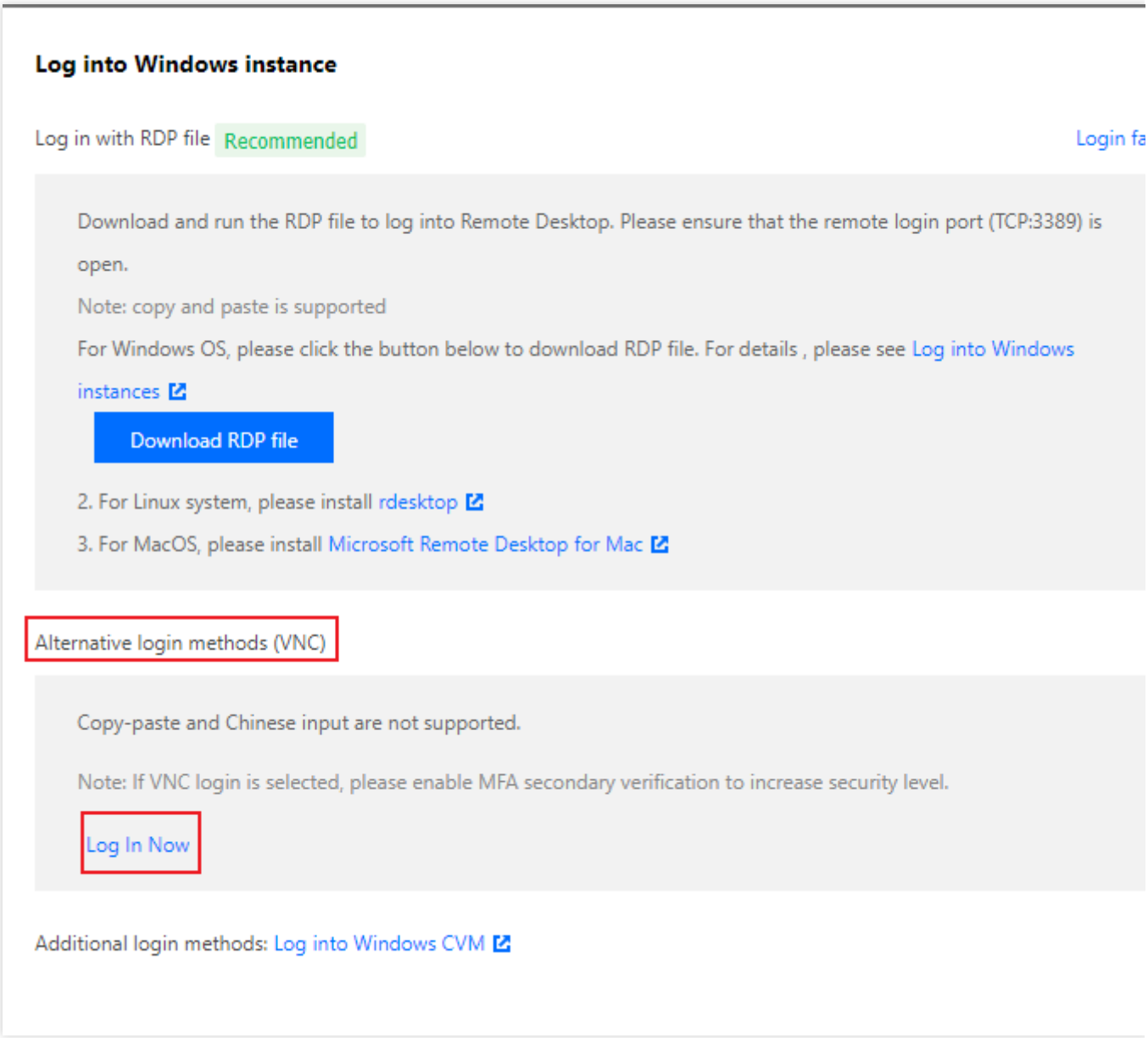
## Langkah-Langkah

1. Login ke Konsol CVM.

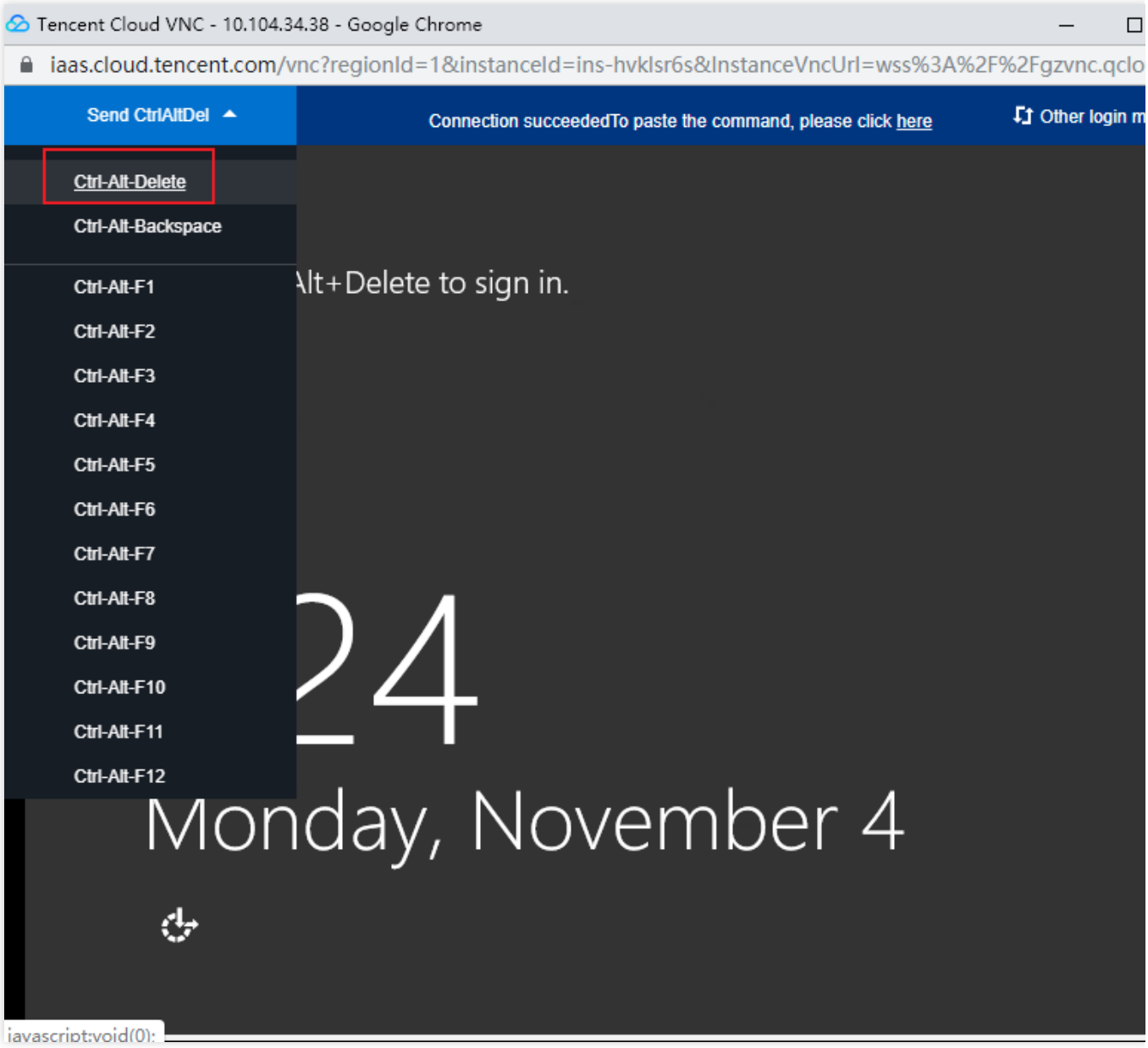
2. Pada halaman manajemen instans, pilih Windows CVM tempat Anda ingin login, lalu klik **Log In** (Login), seperti yang ditunjukkan di bawah ini:




3. Di jendela pop-up **Log into Windows instance** (Login ke instans Windows), pilih **Alternative login methods (VNC)** (Metode login alternatif (VNC)), lalu klik **Log In Now** (Login Sekarang), seperti yang ditunjukkan di bawah ini.




4. Di jendela login, pilih “Send Remote Command” (Kirim Perintah Jarak Jauh) di sudut kiri atas, lalu tekan **Ctrl-Alt-Delete** (Ctrl-Alt-Delete) untuk masuk ke antarmuka login sistem seperti yang ditunjukkan di bawah ini:



# Login ke Instans Windows dari Perangkat Seluler

Waktu update terbaru：2021-12-13 17:07:07

## Ikhtisar

Dokumen ini menjelaskan cara login ke instans Windows dari perangkat seluler yang berbeda menggunakan Microsoft Remote Desktop.

## Perangkat Seluler yang Berlaku

Perangkat iOS dan Android

## Prasyarat

Instans CVM dalam status **Running** (Berjalan).
Anda sudah memiliki akun administrator dan kata sandi untuk login ke instans.
Jika Anda menggunakan kata sandi default sistem untuk login ke instans, buka Pusat Pesan untuk mendapatkan kata sandi terlebih dahulu.
Jika lupa kata sandi, Anda dapat atur ulang sandi instans.
IP publik telah dibeli untuk instans CVM Anda, dan port 3389 terbuka. Port ini terbuka secara default untuk instans CVM yang dibeli dengan konfigurasi cepat.

## Petunjuk

**Keterangan:**
Dokumen ini menggunakan perangkat iOS sebagai contoh. Langkah-langkah untuk perangkat Android hampir sama.
1. Unduh Microsoft Remote Desktop dan mulai.
2. Di halaman **PC** (PC), ketuk **+** (+) di sudut kanan atas, lalu ketuk **Add PC** (Tambahkan PC).
3. Konfigurasikan informasi login untuk menambahkan PC.
**PC name** (Nama PC): alamat IP publik instans CVM Anda. Untuk informasi selengkapnya, lihat Mendapatkan Alamat IP Publik.
**User account** (Akun pengguna): secara default, **Ask when required** (Tanya saat diperlukan) dipilih.

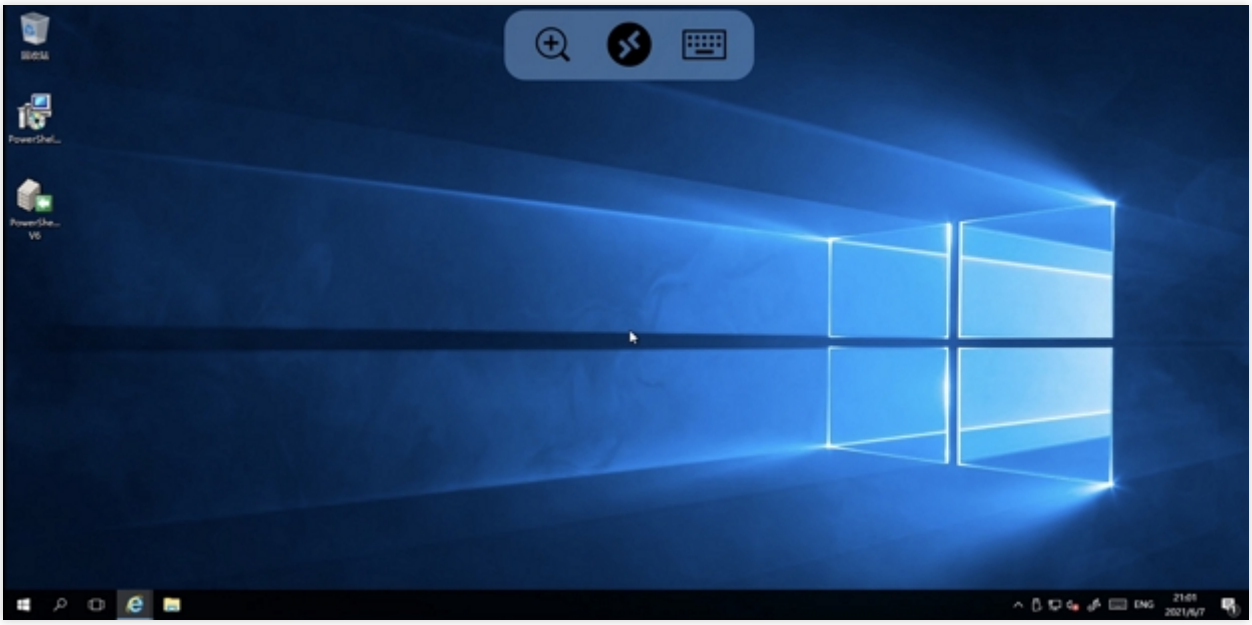
4. Ketuk **Save** (Simpan).

5. Di halaman **PCs** (PC), pilih instans untuk login dan masukkan akun administrator dan kata sandinya.

**User name** (Nama pengguna): masukkan akun administrator `Administrator` .

**Password** (Kata sandi): masukkan kata sandi login instans.

6. Ketuk **Continue** (Lanjutkan). Jika halaman yang ditunjukkan pada gambar berikut ditampilkan, artinya login berhasil.



# Penyesuaian Sumber Daya
# Mengubah Konfigurasi Instans

Waktu update terbaru：2021-12-13 17:07:03

## Ikhtisar

Perangkat keras instans Tencent Cloud CVM dapat disesuaikan dengan cepat dan fleksibel. Dokumen ini menjelaskan metode operasi untuk peningkatan konfigurasi, penurunan versi, dan penyesuaian lintas model.

## Prasyarat

Anda dapat menyesuaikan konfigurasi instans saat dalam status nonaktif atau berjalan. Jika instans sedang berjalan, penyesuaian akan berlaku setelah instans dinonaktifkan dan dimulai ulang secara paksa.
**Keterangan:**
Jika instans telah **shut down** (dimatikan), Anda dapat menyesuaikan konfigurasinya secara langsung melalui konsol.
Jika instans **running** (berjalan), Anda dapat menyesuaikan konfigurasinya secara online dan mengonfirmasi untuk mematikan instans secara paksa. Penyesuaian berlaku setelah instans dimulai ulang.
Anda dapat menyesuaikan konfigurasi instans secara online **in batches** (dalam batch). Jika sebuah instans dalam operasi batch sedang **running** (berjalan), Anda perlu memaksa instans untuk dinonaktifkan. Penyesuaian berlaku setelah instans dimulai ulang.

## Batas dan Dampak

### Batas penyesuaian konfigurasi

Hanya instans **whose system and data disks are both CBS cloud disks** (yang sistem dan disk datanya merupakan disk cloud CBS) yang mendukung penyesuaian konfigurasi.
Peningkatan konfigurasi:
Tidak ada batasan jumlah peningkatan konfigurasi. Peningkatan akan segera berlaku.
Penurunan konfigurasi:
Instans bayar sesuai pemakaian dapat diturunkan beberapa kali kapan saja.
Penyesuaian antar keluarga instans: konfigurasi dapat disesuaikan antar keluarga instans tanpa perlu migrasi data.
Selama penyesuaian konfigurasi, spesifikasi target bergantung pada jenis instans yang disediakan di zona ketersediaan saat ini. Perhatikan batasan berikut:

**Spot instances** (Instans spot) tidak mendukung penyesuaian konfigurasi lintas model.
**Dedicated instances** (Instans khusus) tidak mendukung penyesuaian konfigurasi lintas model. Cakupan penyesuaian tunduk pada sumber daya yang tersisa dari host khusus tempat instans berada.
**Heterogeneous instances such as GPU and FPGA instances** (Instans heterogen seperti instans GPU dan FPGA) tidak dapat digunakan sebagai jenis instans sumber atau target untuk penyesuaian konfigurasi di seluruh kelompok instans.
**Instances configured with a classic network** (Instans yang dikonfigurasi dengan jaringan klasik) tidak dapat disesuaikan dengan instans yang hanya mendukung VPC.
Jika jenis instans target tidak mendukung jenis disk CBS yang dikonfigurasi untuk jenis instans saat ini, konfigurasi tidak dapat disesuaikan.
Jika jenis instans target tidak mendukung jenis citra yang dikonfigurasi untuk jenis instans saat ini, konfigurasi tidak dapat disesuaikan.
Jika jenis instans target tidak mendukung ENI atau kuantitas ENI yang dikonfigurasi untuk jenis instans saat ini, konfigurasi tidak dapat disesuaikan. Untuk informasi selengkapnya, lihat Batas Penggunaan.
Jika jenis instans target tidak mendukung batas bandwidth jaringan publik yang dikonfigurasi untuk jenis instans saat ini, konfigurasi tidak dapat disesuaikan. Untuk informasi selengkapnya, lihat Batas Bandwidth Jaringan Publik.

### Dampak

IP pribadi instans dapat berubah setelah penyesuaian konfigurasi. Dalam hal ini, prompt akan muncul di halaman penyesuaian konfigurasi. Jika tidak, IP pribadi akan tetap sama.

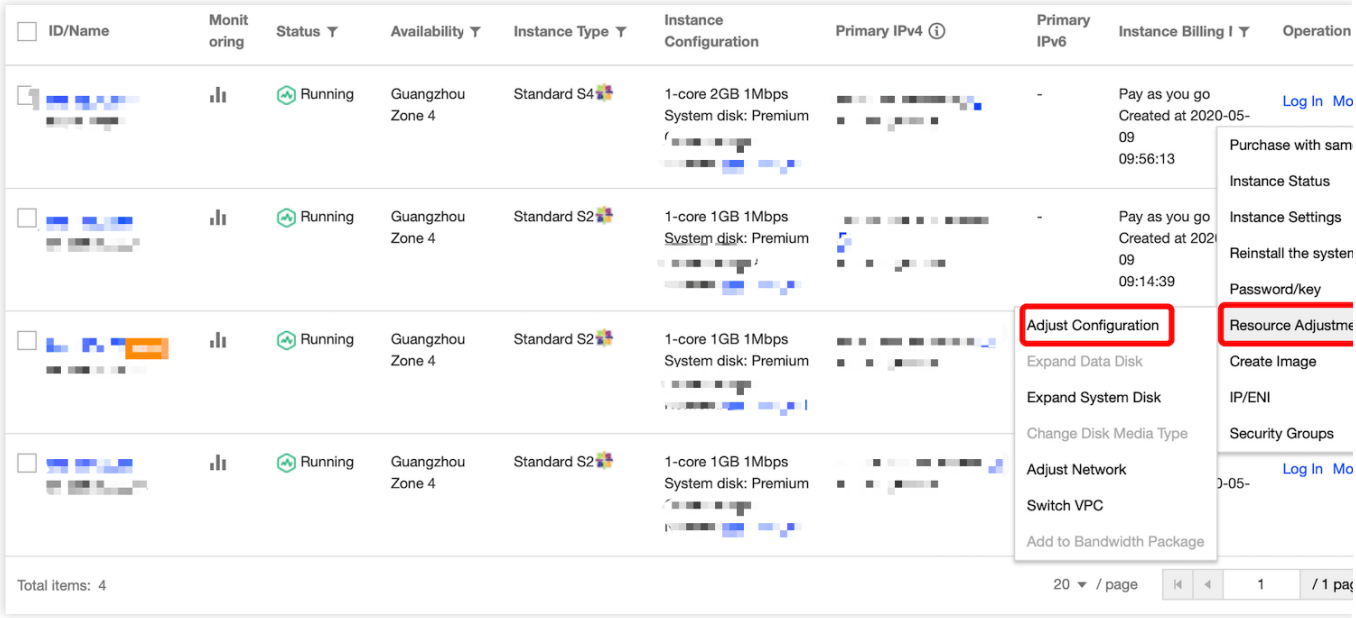
## Petunjuk

**Keterangan:**
Jika bisnis Anda berubah, Anda dapat menyesuaikan konfigurasi instans.
Selama peningkatan konfigurasi, tingkatkan instans CVM Anda sebagaimana mestinya dan bayar biaya yang mungkin dibebankan.
Selama penurunan versi konfigurasi, menonaktifkan paksa dan mulai ulang instans CVM Anda agar konfigurasi baru segera diterapkan.

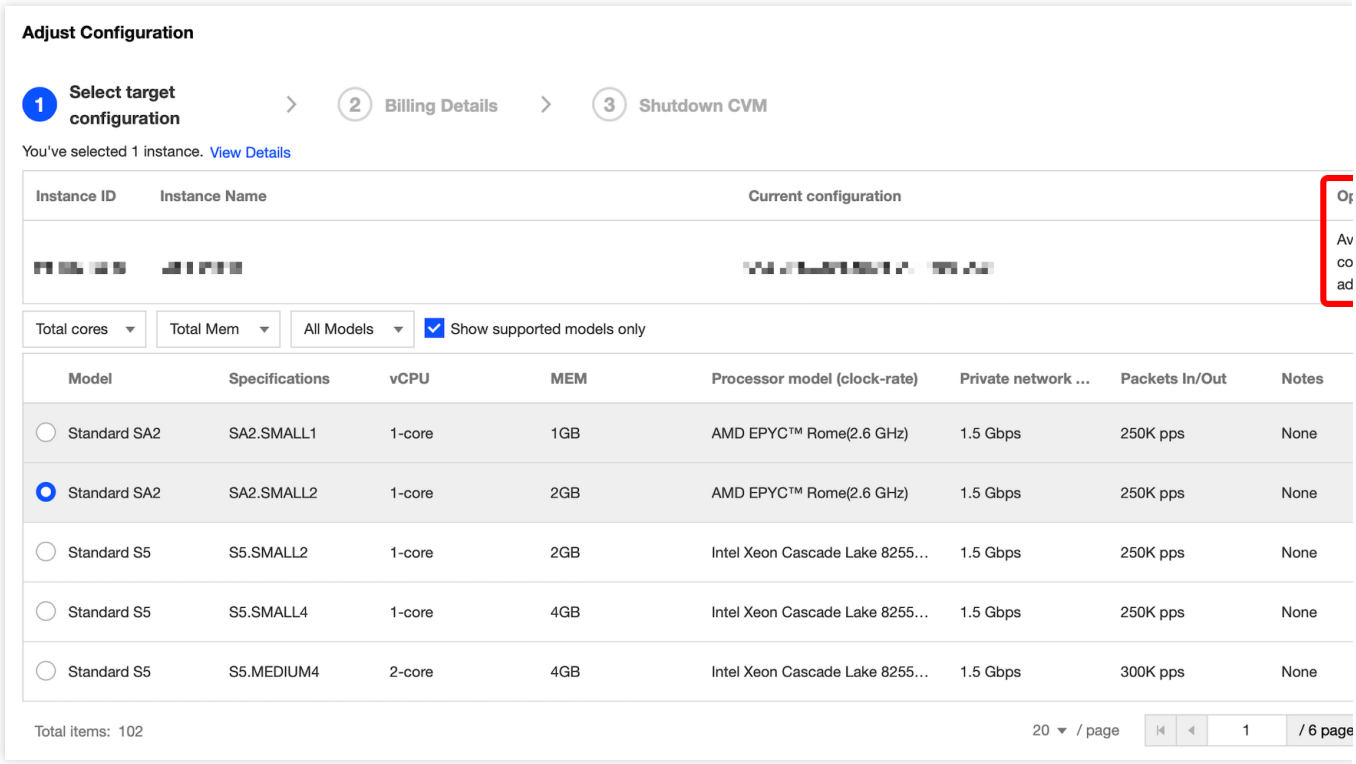
### Penyesuaian konfigurasi melalui konsol

#### Menyesuaikan konfigurasi satu instans

1. Login ke konsol CVM, lalu klik **Instances** (Instans) untuk melihat daftar instans CVM.
2. Temukan instans yang akan disesuaikan dan pilih **More** (Lainnya) > **Resource Adjustment** (Penyesuaian Sumber Daya) > **Adjust Configuration** (Sesuaikan Konfigurasi) di kolom **Operation** (Operasi) di sebelah kanan, seperti yang ditunjukkan pada gambar berikut:

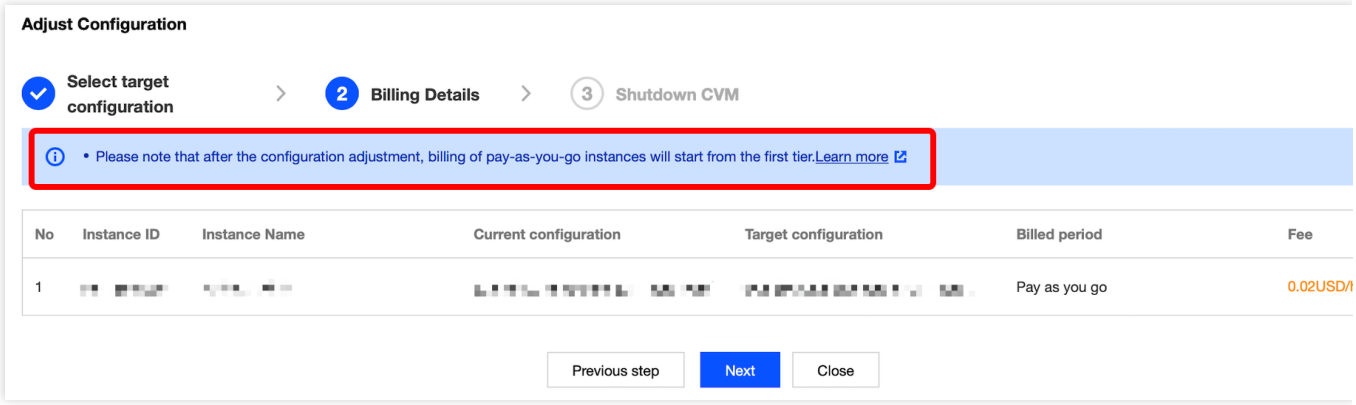



3. Pada langkah "Pilih konfigurasi target", konfirmasikan status dan operasi instans, **select the required model and specifications, confirm the performance parameters** (pilih model dan spesifikasi yang diperlukan, konfirmasi parameter performa), lalu klik **Next** (Selanjutnya), seperti yang ditunjukkan pada gambar berikut:

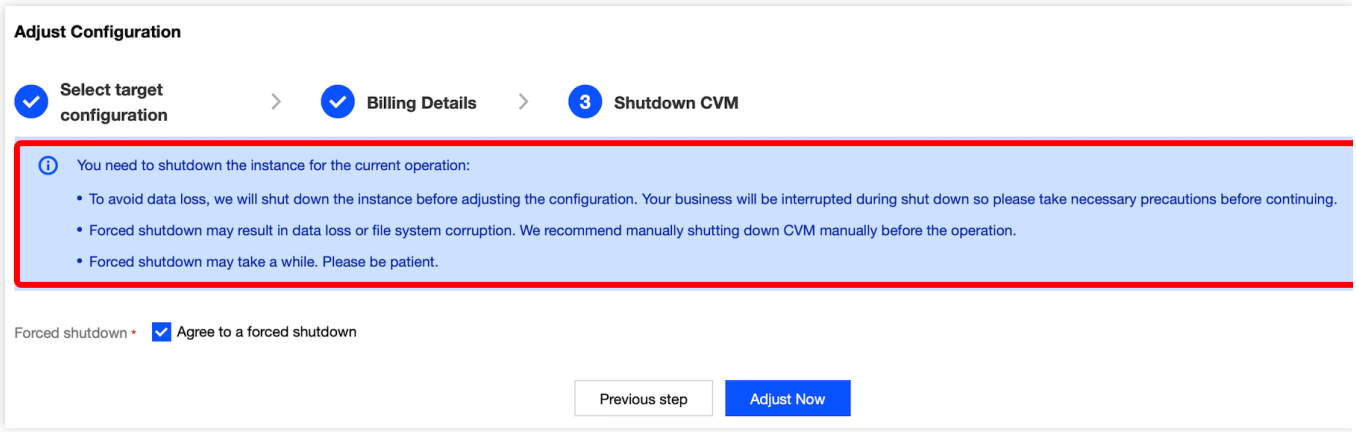



4. Berdasarkan metode penagihan instans, konfirmasi biaya dan klik **Next** (Selanjutnya).
Instans bayar sesuai pemakaian: konfirmasikan jumlah yang akan dibekukan untuk jenis instans baru. Setelah penyesuaian konfigurasi, instans bayar sesuai pemakaian dikenakan biaya mulai dari harga tingkat-Konfirmasi aturan

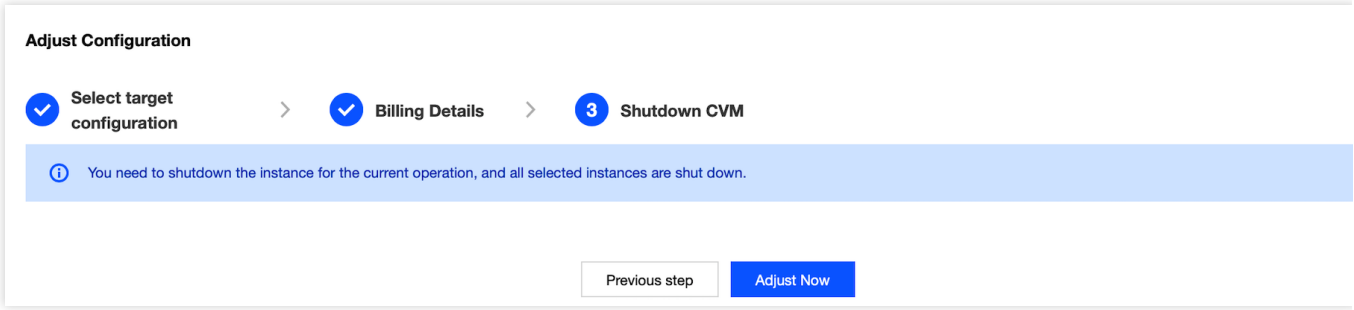
penagihan, seperti yang ditunjukkan pada gambar berikut:




5. Pada langkah "Matikan CVM", baca perintah dengan cermat berdasarkan status instans yang berjalan.
Jika instans saat ini sedang berjalan, baca prompt dengan hati-hati dan pilih "Agree to a forced shutdown"" (Setujui untuk mematikan dengan paksa), seperti yang ditunjukkan pada gambar berikut:




Jika instans saat ini dimatikan, prompt berikut akan muncul:




6. Klik **Adjust Now** (Sesuaikan Sekarang) untuk membuka halaman pesanan dan menyelesaikan pembayaran.

## Penyesuaian konfigurasi melalui API

Anda dapat menggunakan ResetInstancesType API untuk menyesuaikan konfigurasi instans. Untuk informasi selengkapnya, lihat dokumentasi API ResetInstancesType.

# Menyesuaikan Konfigurasi Jaringan

Waktu update terbaru：2021-12-13 17:07:03

## Ikhtisar

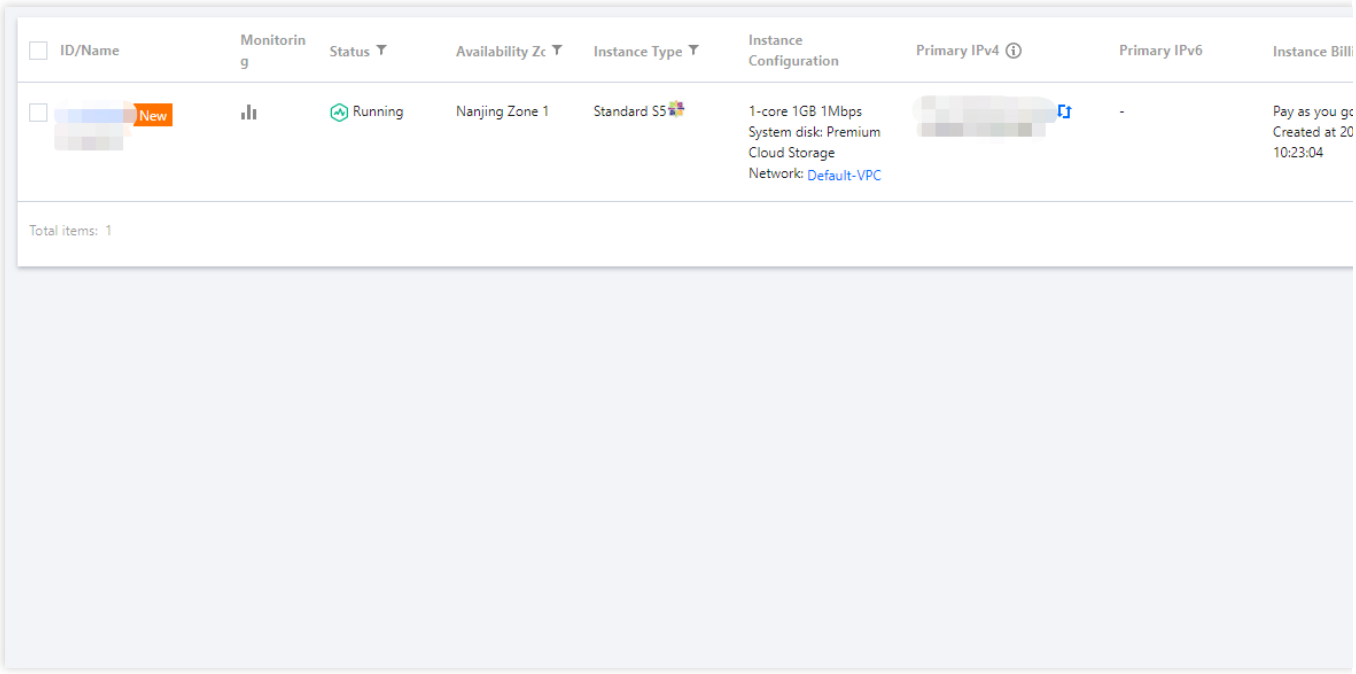
Tencent Cloud memungkinkan Anda mengubah mode penagihan jaringan publik atau bandwidth jaringan publik sesuai kebutuhan. Perubahan akan segera berlaku. Untuk mempelajari selengkapnya tentang batasan dan harga, lihat Menyesuaikan Penagihan Jaringan Publik.

## Petunjuk

### Mengubah mode penagihan

Tencent Cloud menyediakan dua paket penagihan jaringan: tagihan per lalu lintas dan tagihan per bandwidth. Anda dapat beralih di antara mereka di konsol seperti yang diinstruksikan di bawah ini:

1. Login ke konsol CVM. Di bagian atas halaman **Instances** (Instans), pilih wilayah tempat instans CVM target berada.
2. Temukan instans CVM target, lalu klik **More** (Lainnya) > **Resource Adjustment** (Penyesuaian Sumber Daya) > **Adjust Network** (Sesuaikan Jaringan) di bawah kolom **Operation** (Operasi), seperti yang ditunjukkan di bawah ini.



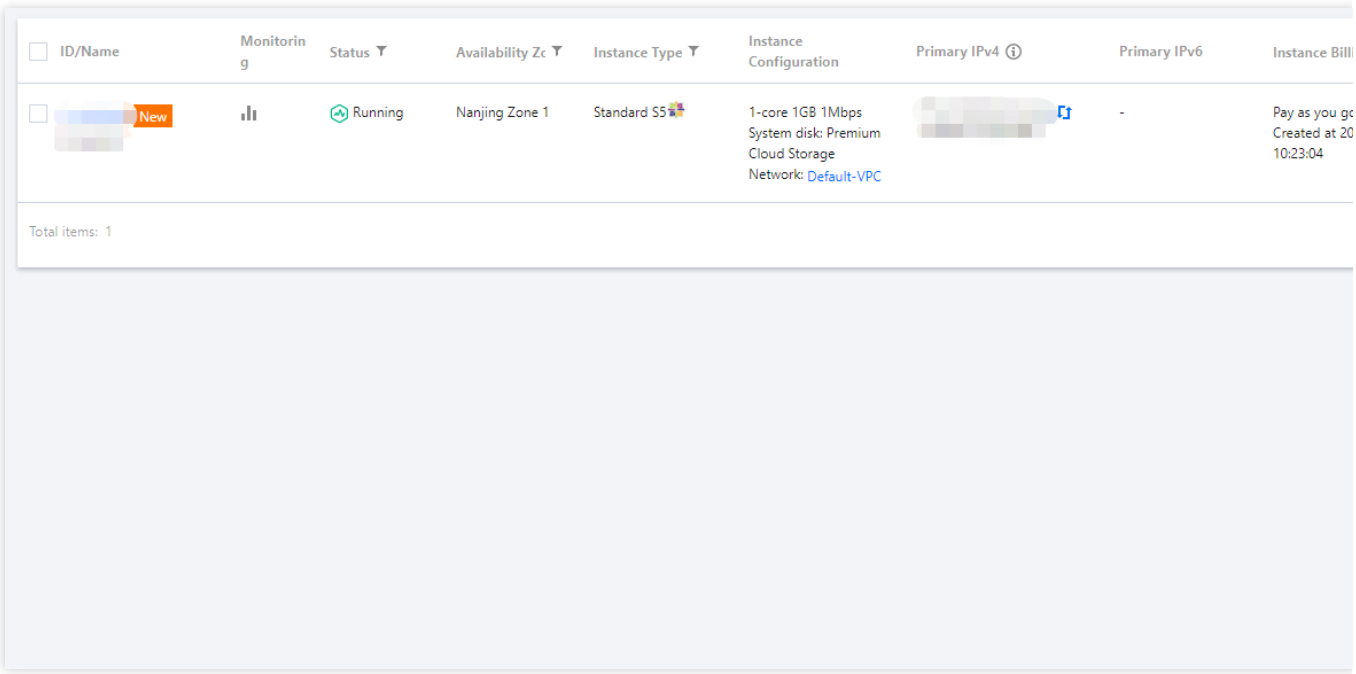

3. Pada kotak dialog pop-up, pilih mode penagihan jaringan yang ingin Anda gunakan, dan klik **Confirm** (Konfirmasi).

**Menyesuaikan bandwidth jaringan publik**

Dokumen ini menjelaskan cara menyesuaikan batas bandwidth instans CVM.

1. Login ke konsol CVM. Di bagian atas halaman **Instances** (Instans), pilih wilayah tempat instans CVM target berada.

2. Temukan instans CVM target, lalu klik **More** (Lainnya) > **Resource Adjustment** (Penyesuaian Sumber Daya) > **Adjust Network** (Sesuaikan Jaringan) di bawah kolom **Operation** (Operasi), seperti yang ditunjukkan di bawah ini.




3. Pada kotak dialog pop-up, pilih batas bandwidth baru, lalu klik **Confirm** (Konfirmasi).

**Keterangan:**

Untuk informasi selengkapnya tentang batas bandwidth, lihat Batas Bandwidth Jaringan Publik.

# Dokumentasi

Menyesuaikan Penagihan Jaringan Publik

Penagihan Jaringan Publik

Mode Penagihan

Batas Bandwidth Jaringan Publik

# Info Kueri

# Info Pemantauan Instans Kueri

Waktu update terbaru：2021-12-13 17:07:03

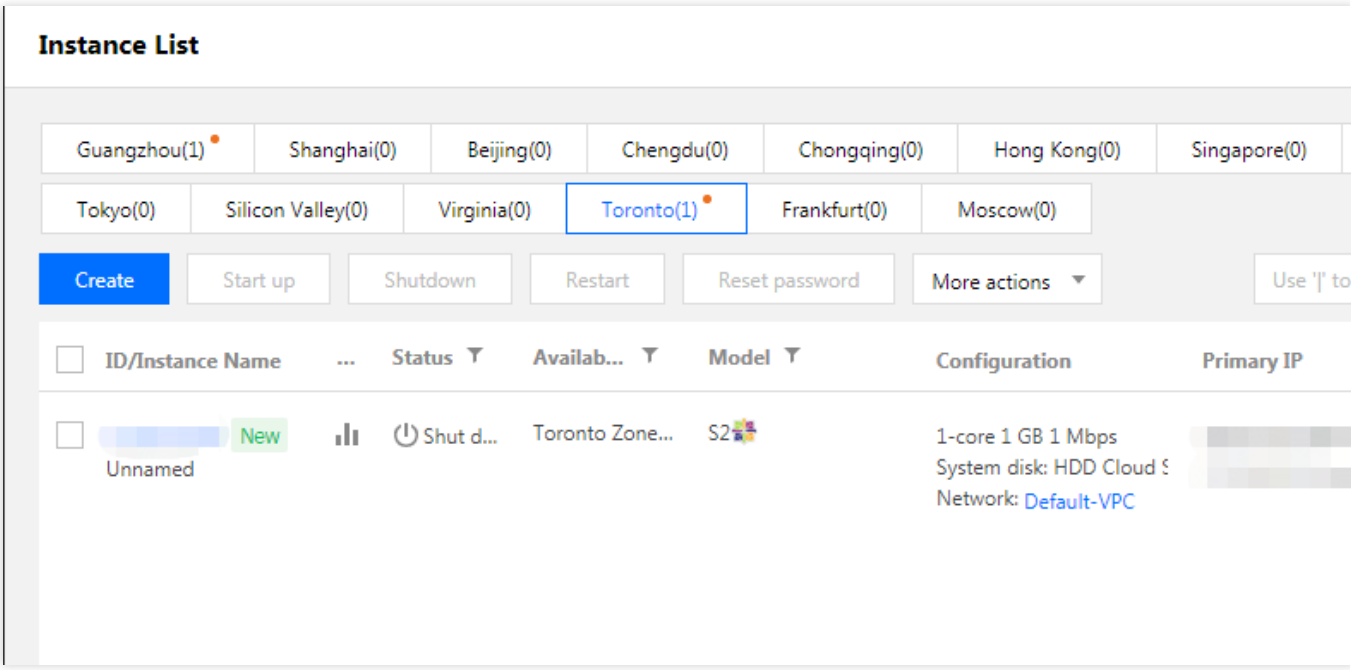
## Skenario

Tencent Cloud menyediakan dua opsi untuk melihat informasi pemantauan instans CVM:
Konsol Cloud Monitor
Halaman **Instance Details** (Detail Instans) di konsol CVM
Untuk melihat informasi pemantauan lalu lintas jaringan publik, buka Pemantau Lalu Lintas.

## Petunjuk

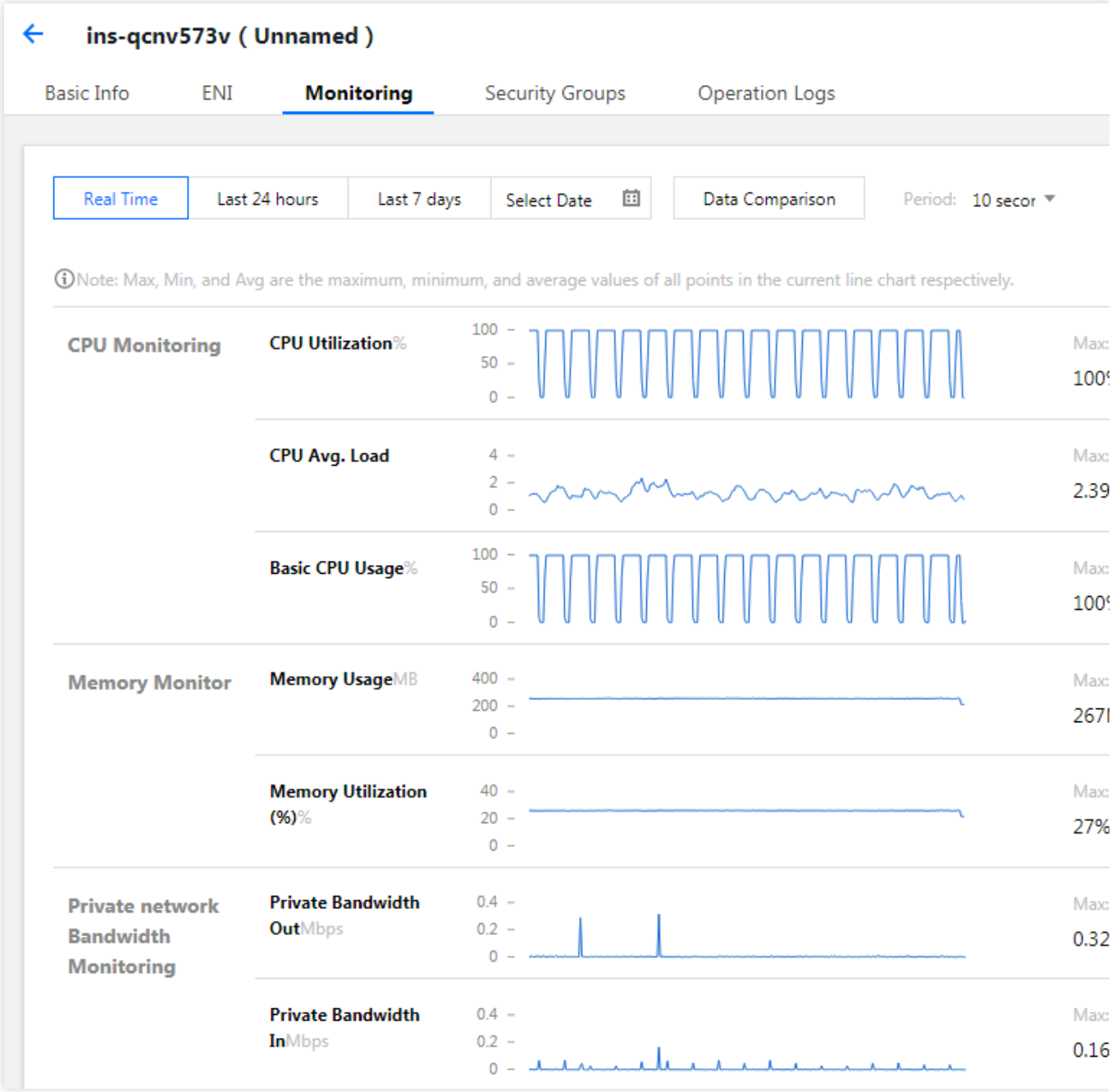
### Melihat informasi pemantauan instans di konsol Cloud Monitor

1. Login ke konsol Cloud Monitor CVM.
2. Pilih wilayah tempat instans yang informasi pemantauannya akan dilihat berada, seperti yang ditunjukkan pada gambar berikut.



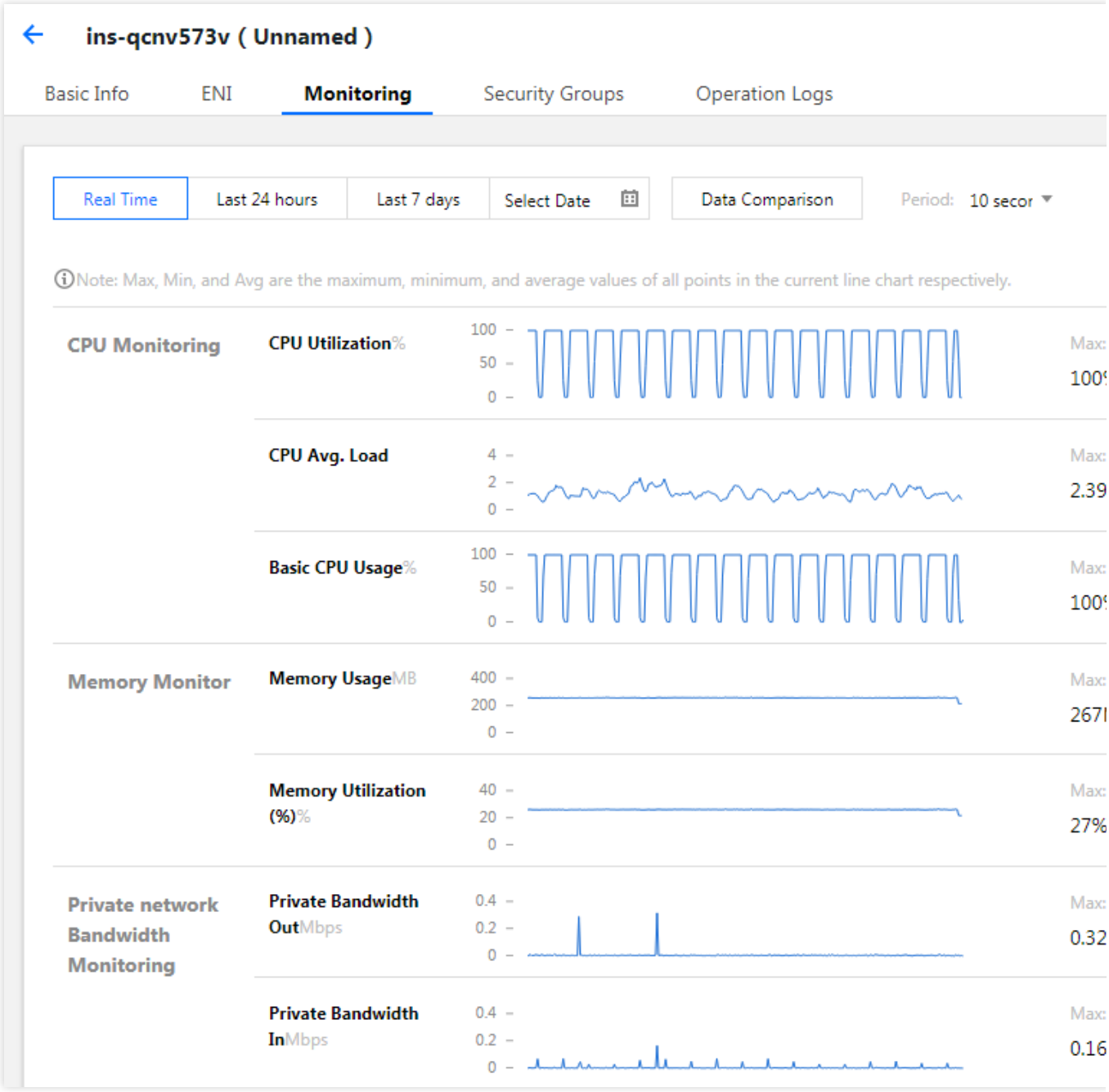

3. Klik ID instans untuk membuka halaman **Monitoring** (Pemantauan). Pada halaman ini, Anda dapat melihat metrik CPU, memori, bandwidth jaringan pribadi, bandwidth jaringan publik, dan penggunaan disk dari CVM, seperti yang

ditunjukkan pada gambar berikut.




## Melihat informasi pemantauan instans di konsol CVM

1. Login ke konsol CVM.
2. Pilih wilayah tempat instans yang informasi pemantauannya akan dilihat berada.
3. Klik ID instans untuk membuka halaman **Instance Details** (Detail Instans).
4. Klik tab **Monitoring** (Pemantauan) untuk membuka halaman **Monitoring** (Pemantauan). Pada halaman ini, Anda dapat melihat metrik CPU, memori, bandwidth jaringan pribadi, bandwidth jaringan publik, dan penggunaan disk dari CVM, seperti yang ditunjukkan pada gambar berikut.



# Mengkueri Metadata Instans

Waktu update terbaru：2021-12-13 17:07:03

Metadata instans mengacu pada data yang relevan dengan sebuah instans. Metadata ini dapat digunakan untuk mengonfigurasi atau mengelola instans yang sedang berjalan.

**Keterangan:**

Meskipun metadata instans hanya dapat diakses setelah login, data belum dienkripsi. Siapa pun yang mengakses instans dapat melihat metadatanya. Dengan demikian, Anda harus mengambil tindakan yang tepat untuk melindungi data sensitif.

## Ikhtisar

Tencent Cloud menyediakan metadata berikut:

| Nama | Deskripsi | Versi |
|---|---|---|
| instance-id | ID Instans | 1.0 |
| instance-name | Nama instans | 1.0 |
| uuid | ID instans unik | 1.0 |
| local-ipv4 | Alamat IP pribadi instans | 1.0 |
| public-ipv4 | Alamat IP publik instans | 1.0 |
| mac | Alamat MAC perangkat eth0 instans | 1.0 |
| penempatan/wilayah | Wilayah instans | 2017-09-19 |
| penempatan/zona | Zona ketersediaan instans | 2017-09-19 |
| network/interfaces/macs/${mac}/mac | Alamat MAC dari antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/primary-local-ipv4 | IP pribadi utama dari antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/public-ipv4s | Alamat IP publik dari antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/vpc-id | ID VPC dari antarmuka jaringan instans | 2017-09-19 |

| | | |
|---|---|---|
| network/interfaces/macs/${mac}/subnet-id | ID Subnet dari antarmuka jaringan instans | 2017-09-19 |
| network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/gateway | Alamat gateway antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/local-ipv4 | Alamat IP pribadi dari antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/public-ipv4 | Alamat IP publik dari antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/public-ipv4-mode | Mode jaringan publik dari antarmuka jaringan instans | 1.0 |
| network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/subnet-mask | Subnet mask dari antarmuka jaringan instans | 1.0 |
| pembayaran/jenis tagihan | Paket penagihan instans | 2017-09-19 |
| pembayaran/waktu pembuatan | Waktu pembuatan instans | 2017-09-19 |
| pembayaran/waktu penghentian | Waktu penghentian instans | 2017-09-19 |
| app-id | AppID dari pemilik instans | 2017-09-19 |
| as-group-id | ID grup penskalaan otomatis dari instans | 2017-09-19 |
| spot/waktu penghentian | Spot waktu penghentian instans | 2017-09-19 |
| /meta-data/instans/instans-type | Jenis instans | 2017-09-19 |
| /instans/image-id | ID citra instans | 2017-09-19 |
| /instance/security-group | Informasi grup keamanan yang terikat pada instans | 2017-09-19 |
| /instans/bandwidth-limit-egress | Batas bandwidth keluar jaringan pribadi instans, dalam Kbit/d | 2019-09-29 |

| | | |
|---|---|---|
| /instance/bandwidth-limit-ingress | Batas bandwidth masuk jaringan pribadi instans, dalam Kbit/d | 2019-09-29 |
| /cam/security-credentials/${role-name} | Kredensial sementara yang dibuat oleh kebijakan peran CAM, yang hanya dapat diperoleh jika instans dikaitkan dengan peran CAM. Ubah `${role-name}` menjadi nama peran CAM yang sebenarnya; jika tidak, `404` akan ditampilkan | 2019-12-11 |

**Keterangan:**

Bidang `${mac}` dan `${local-ipv4}` pada tabel di atas menunjukkan alamat MAC dan alamat IP pribadi dari antarmuka jaringan yang ditentukan untuk masing-masing instans.

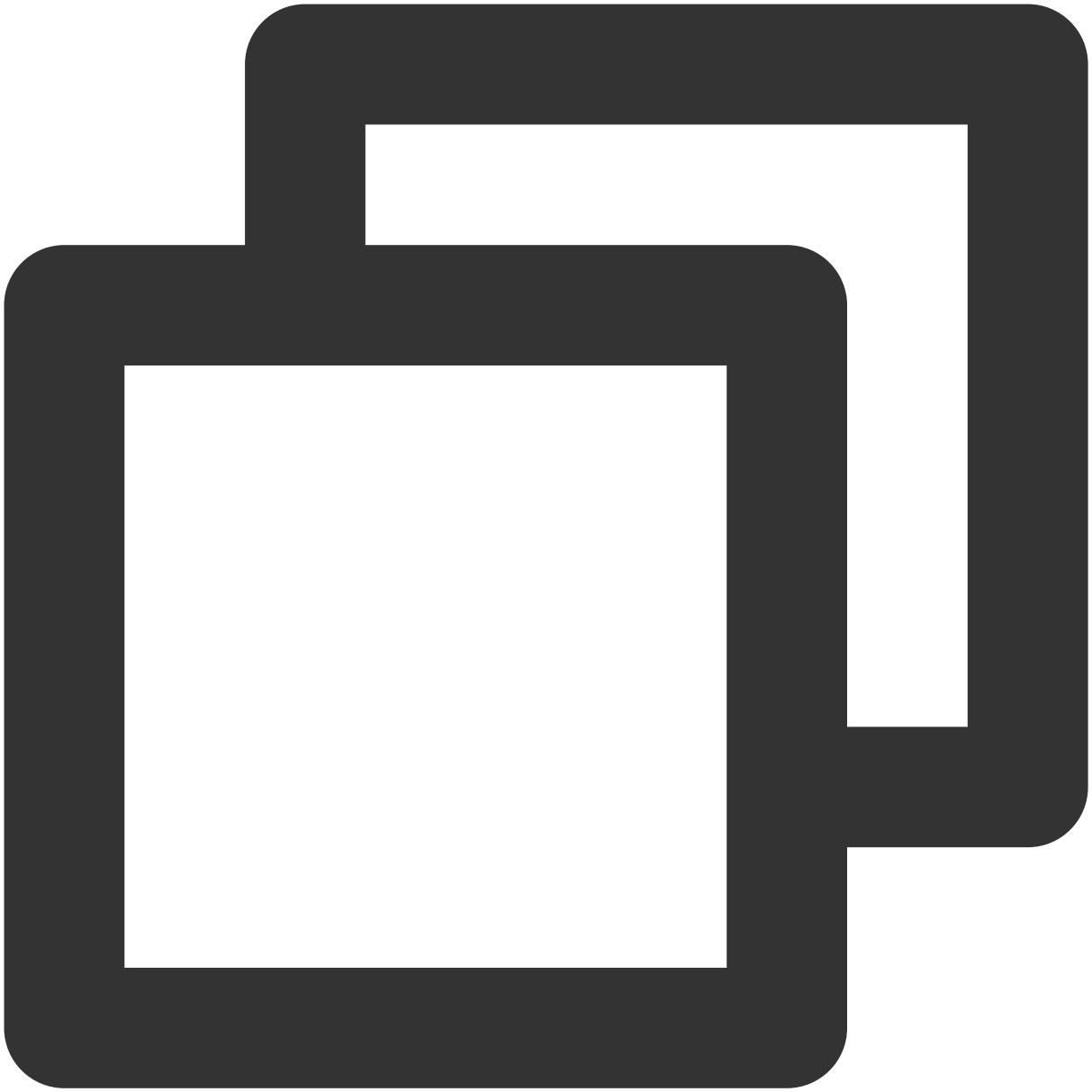
Alamat URL tujuan permintaan peka huruf besar/kecil. Anda harus membuat alamat URL tujuan permintaan baru sesuai dengan hasil permintaan yang ditampilkan.

Data `penempatan` yang ditampilkan diubah dalam versi baru. Untuk menggunakan data di versi sebelumnya, tentukan jalur versi sebelumnya atau biarkan jalur versi kosong untuk mengakses data versi 1.0. Untuk informasi selengkapnya tentang data `penempatan` yang ditampilkan, lihat Wilayah dan Zona Ketersediaan.

# Mengkueri Metadata Instans

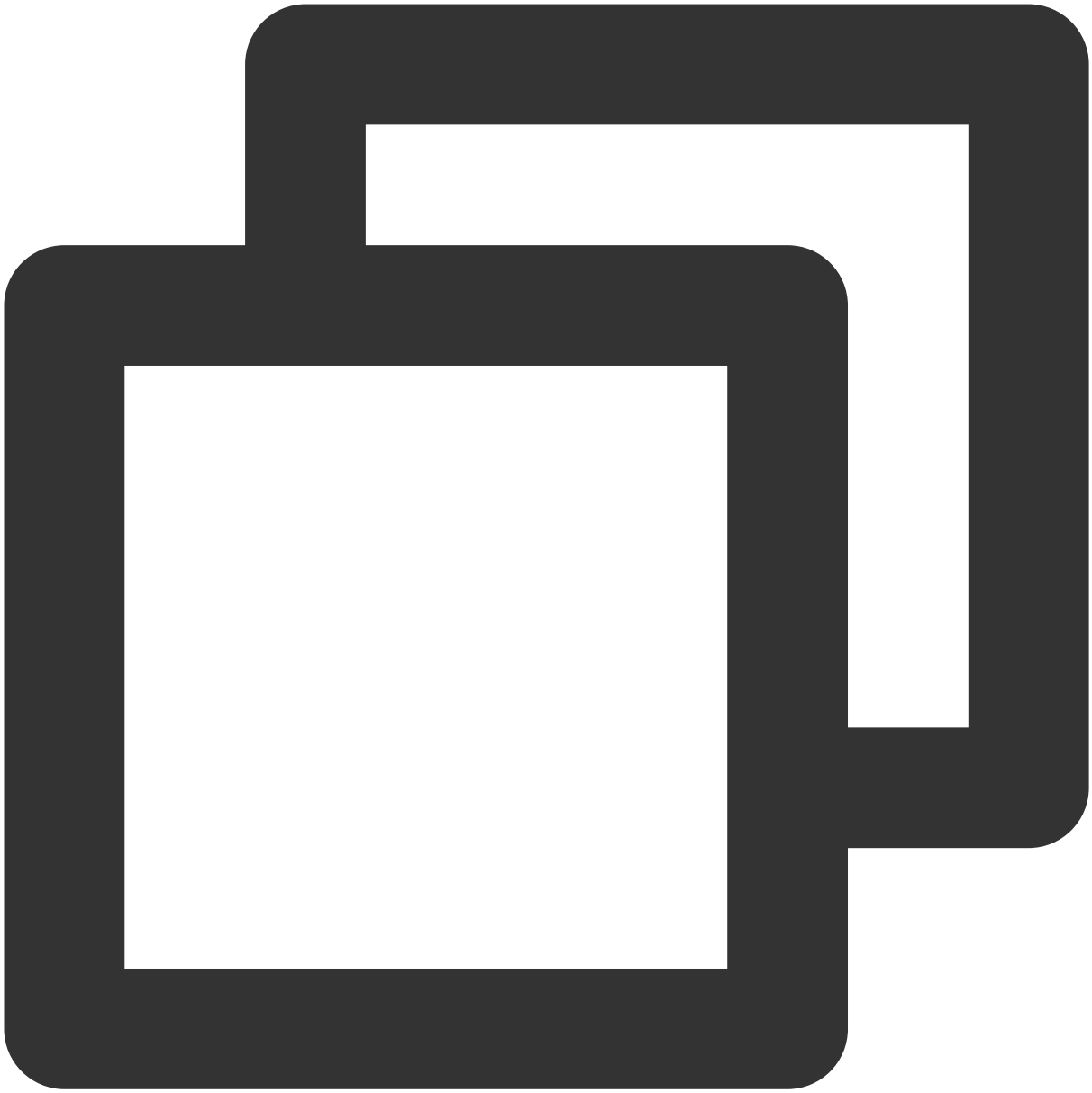
Setelah login ke instans, Anda dapat mengakses metadata seperti alamat IP lokal dan alamat IP publik untuk mengelola koneksi dengan aplikasi eksternal.

Untuk melihat semua metadata instans dalam instans yang sedang berjalan, gunakan URI berikut:



```
http://metadata.tencentyun.com/latest/meta-data/
```

Anda dapat mengakses metadata dengan menggunakan alat cURL atau permintaan HTTP GET, misalnya:



```
curl http://metadata.tencentyun.com/latest/meta-data/
```

Untuk sumber daya yang tidak ada, kode kesalahan HTTP "404 - Not Found" (404 - Tidak Ditemukan) akan ditampilkan.

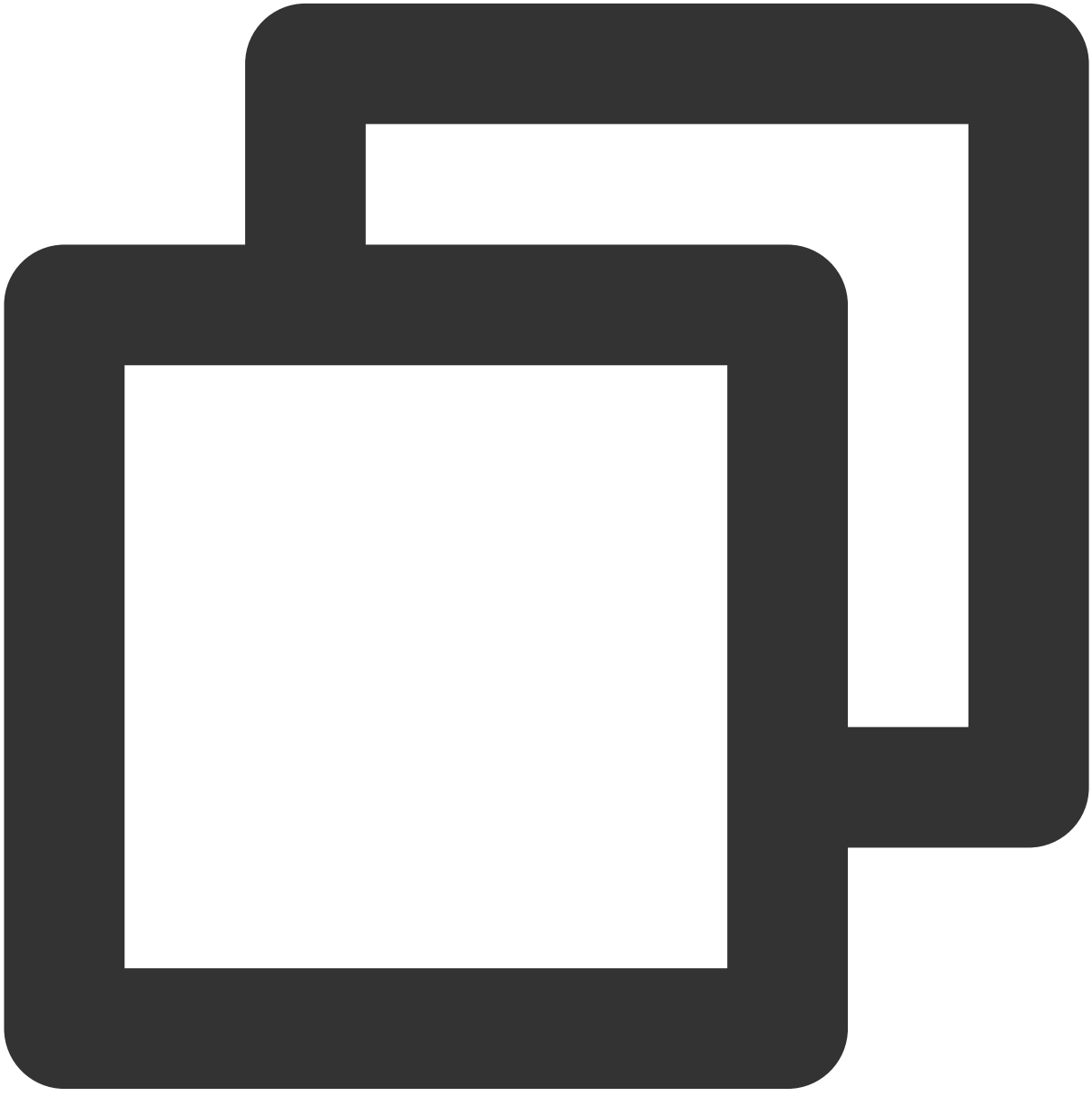
Untuk mengoperasikan metadata instans, silakan login ke instans terlebih dahulu. Untuk informasi selengkapnya, lihat Login ke Instans Windows Menggunakan RDP (Direkomendasikan) dan Login ke Instans Linux Menggunakan Metode Login Standar.

### Contoh kueri metadata

Contoh berikut menunjukkan cara mendapatkan versi metadata.

**Perhatian:**

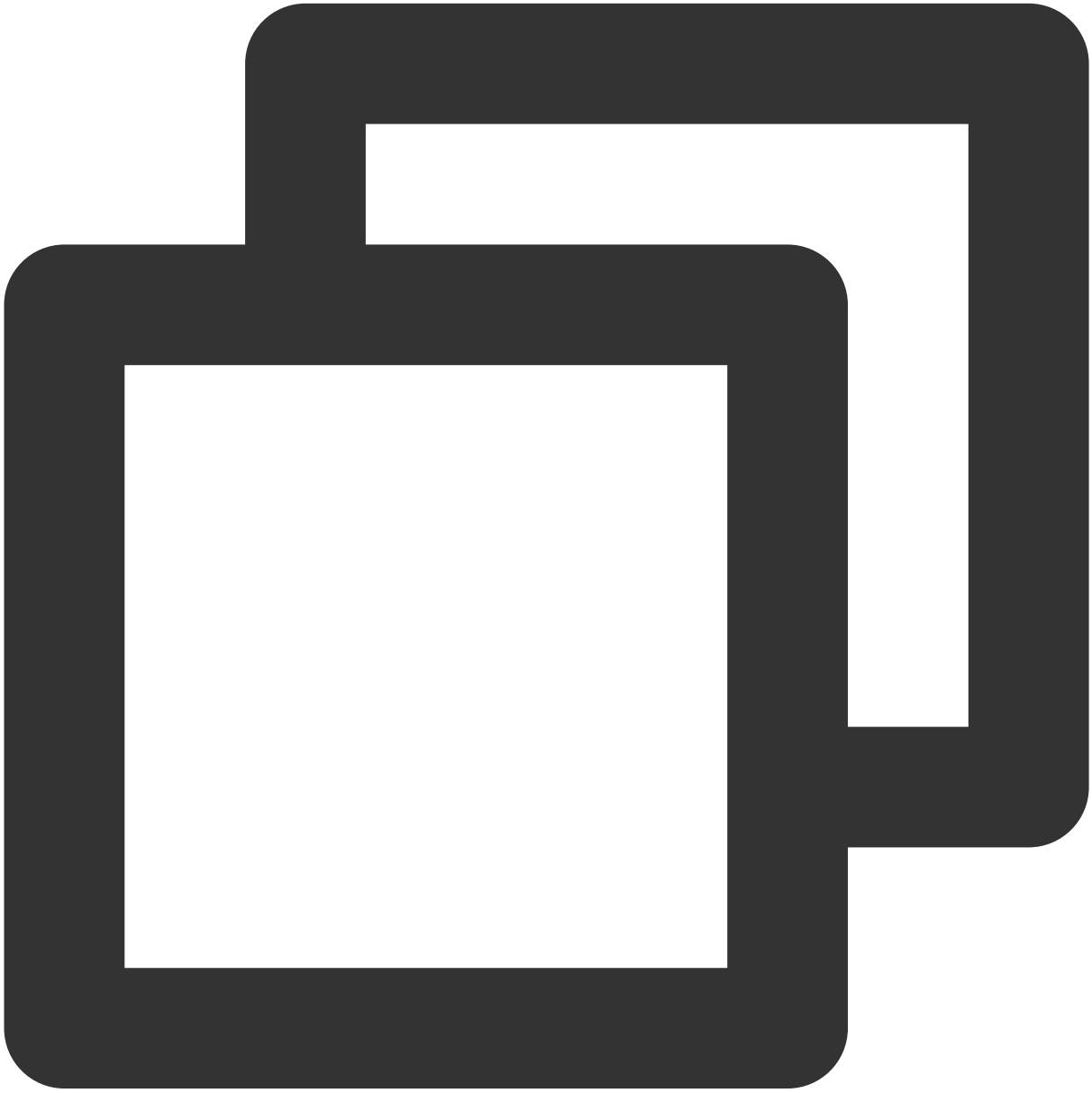
Saat Tencent Cloud memodifikasi jalur akses metadata atau data yang ditampilkan, versi metadata baru akan dirilis. Jika aplikasi atau skrip Anda bergantung pada struktur atau data yang dikembalikan dari versi sebelumnya, Anda dapat mengakses metadata menggunakan versi sebelumnya yang ditentukan. Jika tidak ada versi yang ditentukan, versi 1.0 diakses secara default.



```
[qcloud-user]# curl http://metadata.tencentyun.com/
1.0
2017-09-19
```

```
terbaru
meta-data
```

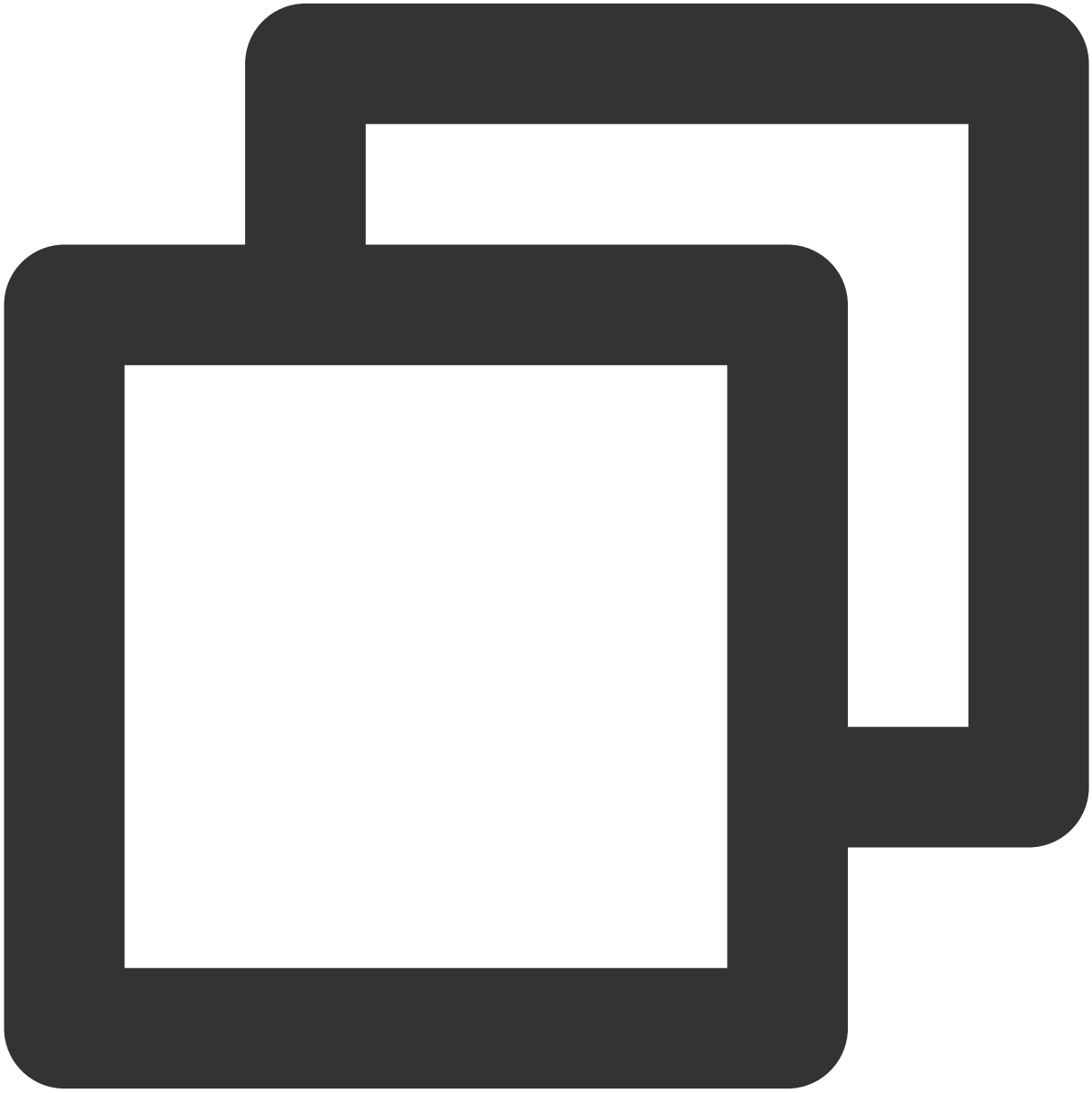
Contoh berikut menunjukkan cara melihat direktori root metadata. Baris yang diakhiri dengan `/` mewakili direktori dan baris lainnya mewakili data yang diakses. Untuk deskripsi data yang diakses, lihat bagian **Overview** (Ikhtisar) yang dijelaskan di atas.



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/
instance-id
instance-name
local-ipv4
```

```
mac
network/
placement/
public-ipv4
uuid
```

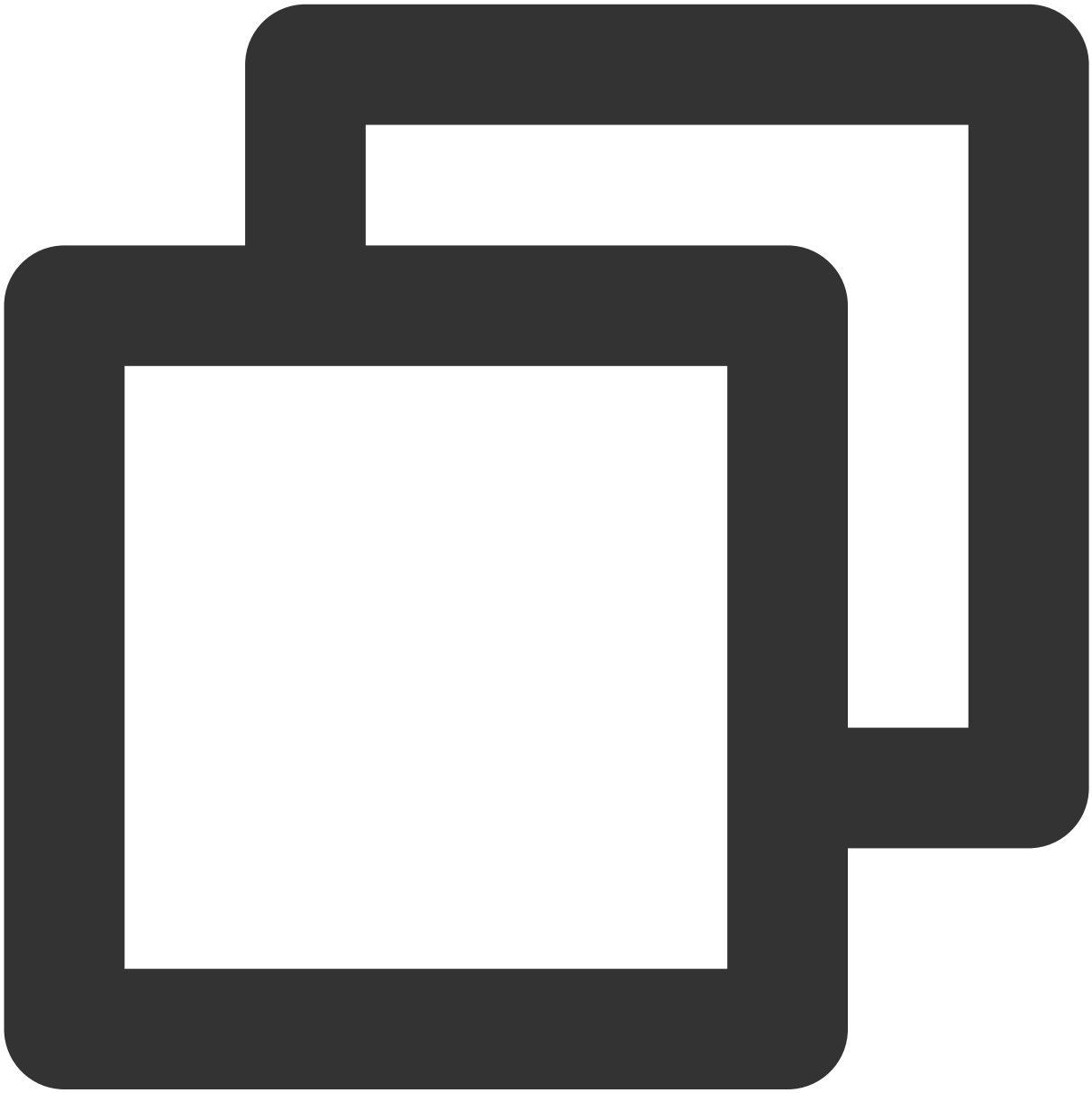
Contoh berikut menunjukkan cara mendapatkan informasi lokasi fisik dari instans. Untuk hubungan antara data yang dikembalikan dan lokasi fisik, lihat Wilayah dan Zona Ketersediaan.



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/regio
ap-guangzhou
```

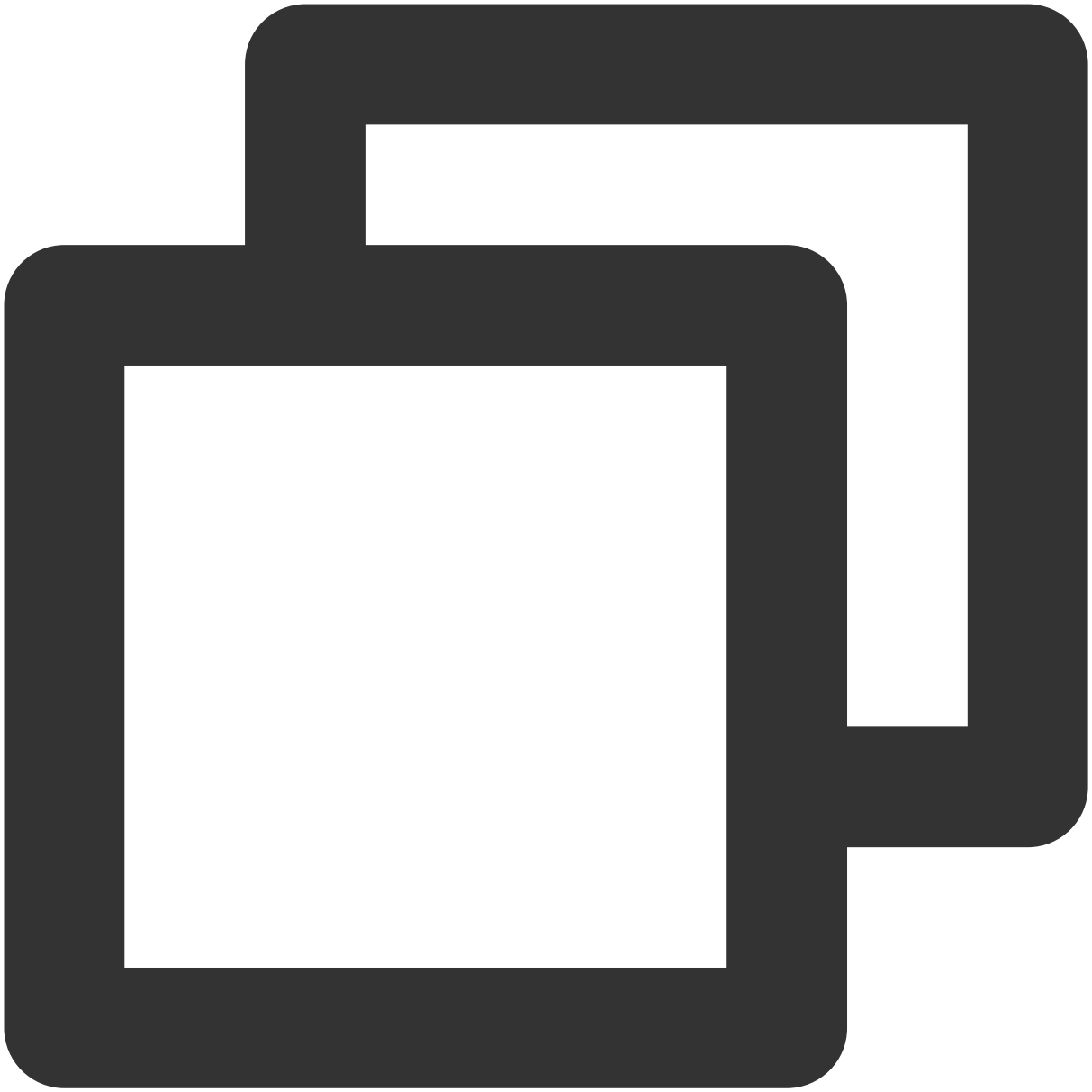
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/zone
ap-guangzhou-3
```

Contoh berikut menunjukkan cara mendapatkan alamat IP pribadi instans. Jika instans memiliki beberapa ENI, alamat jaringan perangkat eth0 akan ditampilkan.



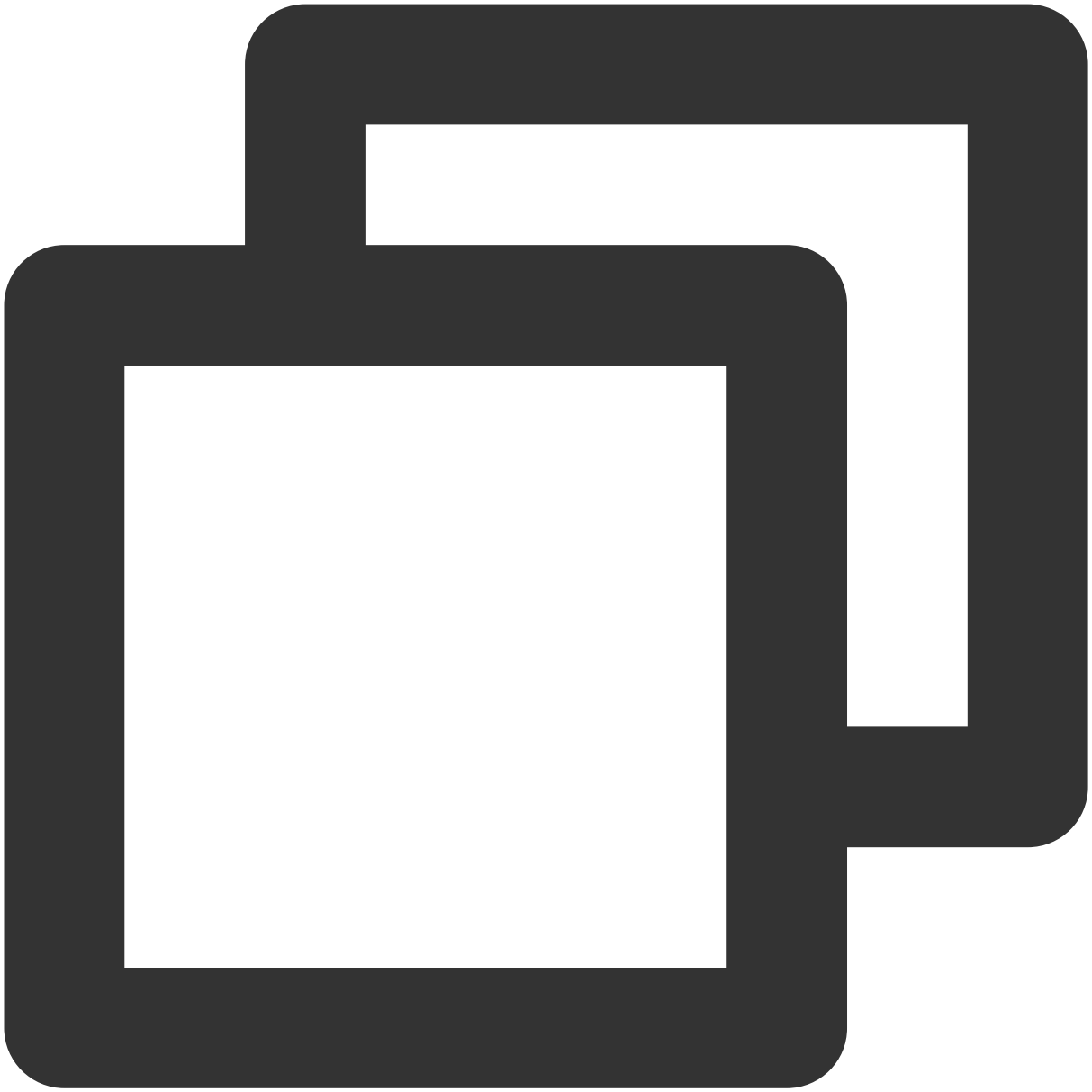
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/local-ipv4
10.104.13.59
```

Contoh berikut menunjukkan cara mendapatkan alamat IP publik instans.



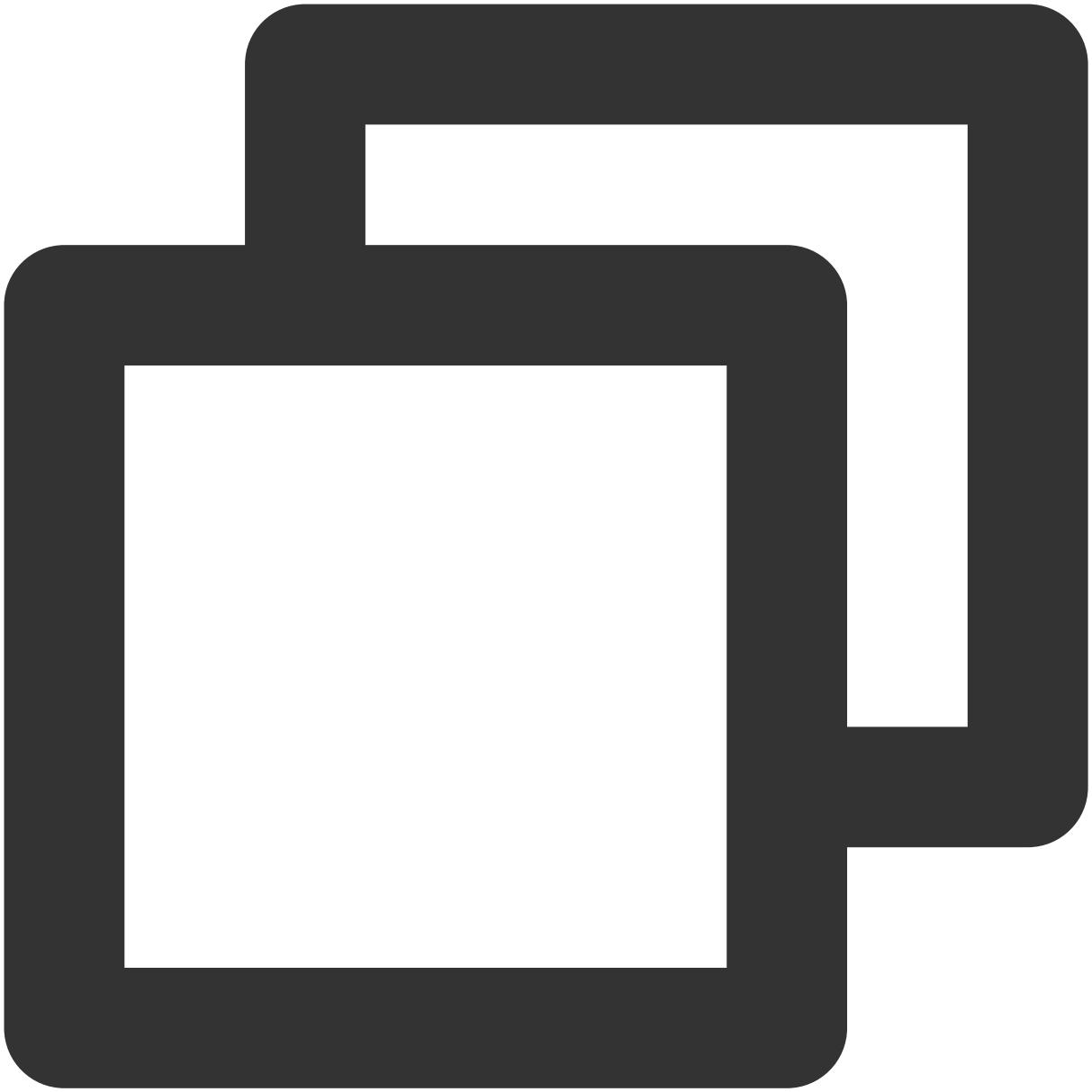
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/public-ipv4
139.199.11.29
```

Contoh berikut menunjukkan cara mendapatkan ID instans. ID instans digunakan untuk mengidentifikasi instans secara unik.



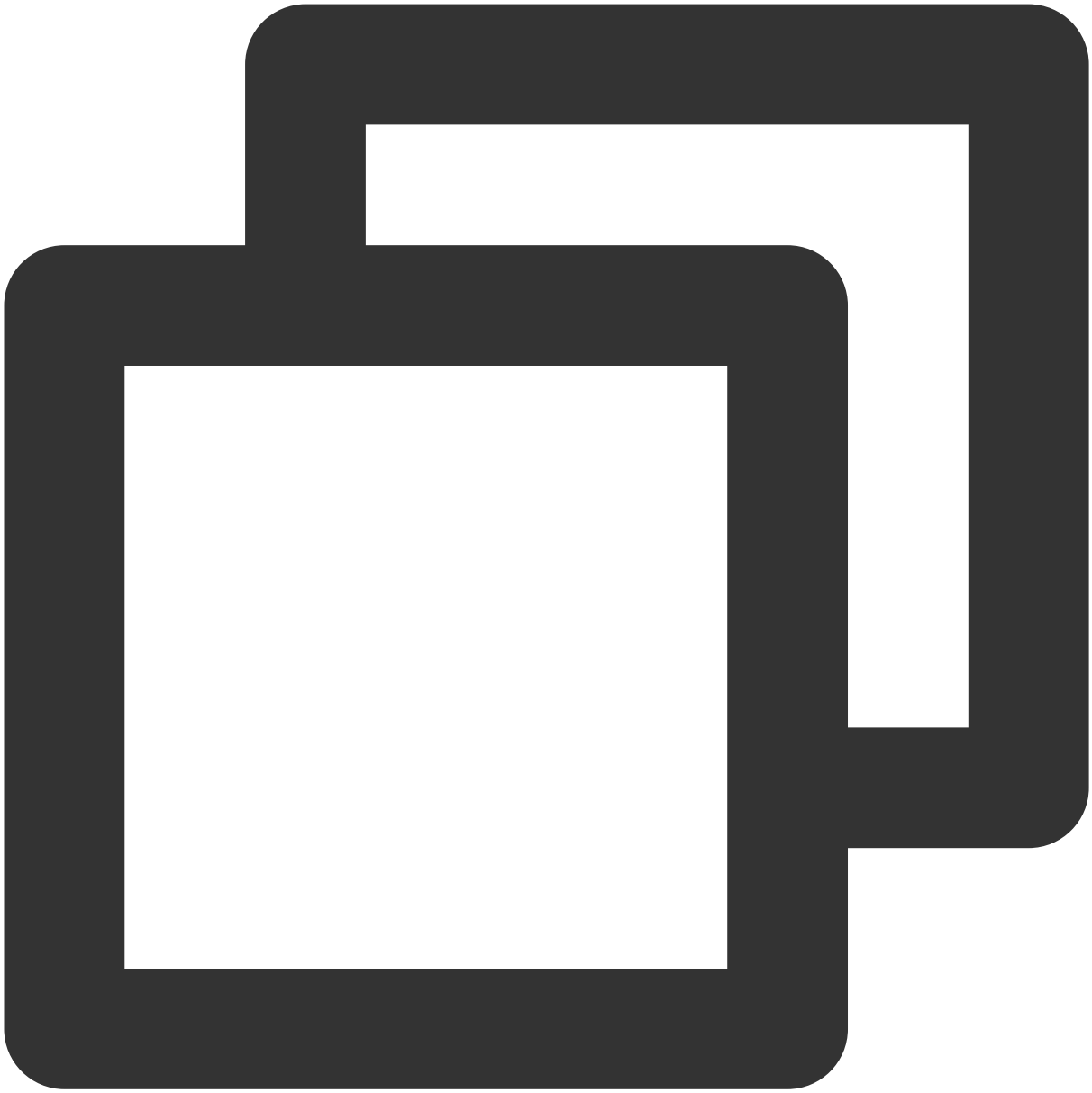
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/instance-id
ins-3g445roi
```

Contoh berikut menunjukkan cara mengkueri instans UUID. UUID instans juga dapat digunakan sebagai pengidentifikasi unik instans, tetapi sebaiknya gunakan ID instans untuk mengidentifikasi instans.



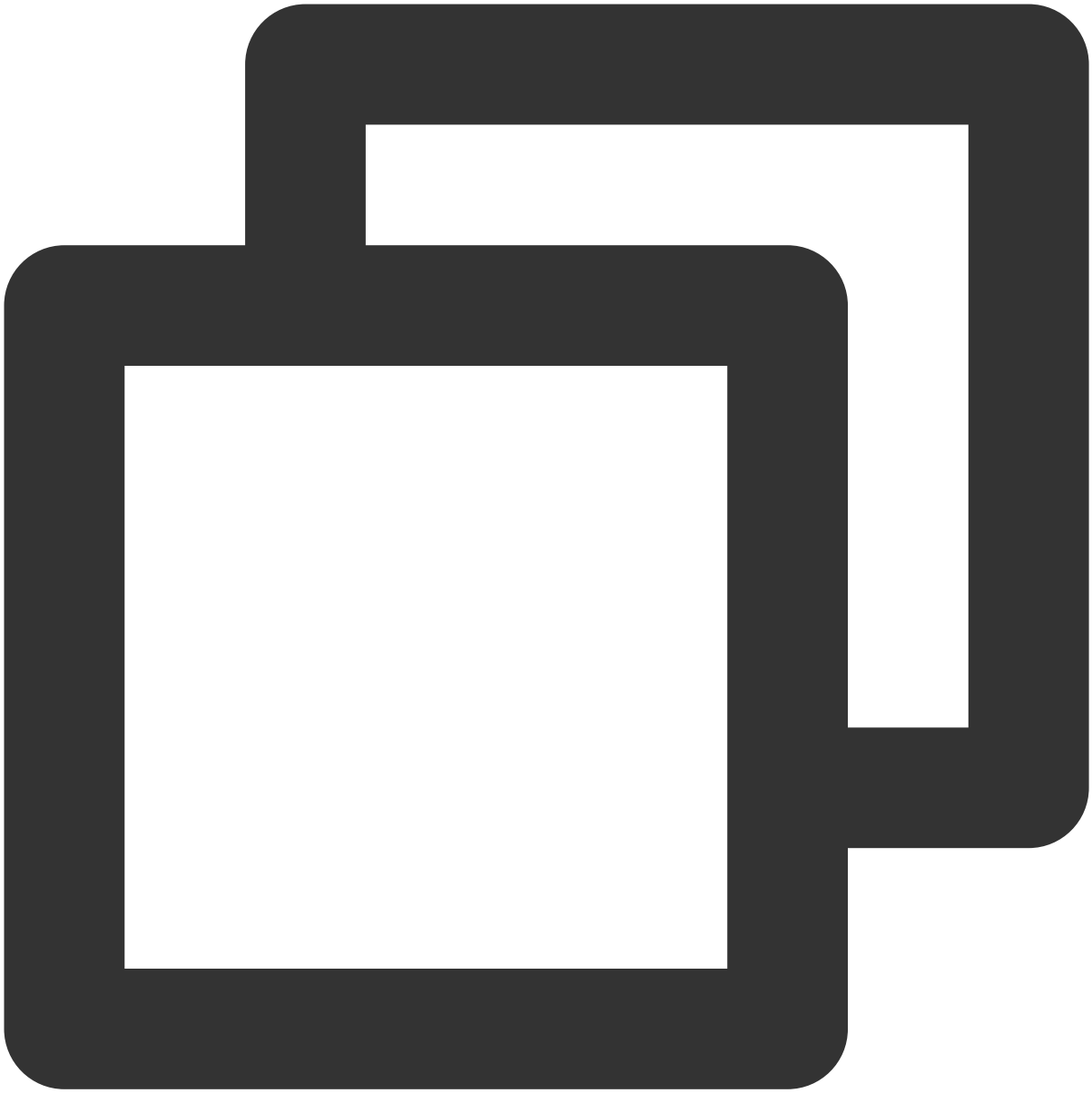
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/uuid
cfac763a-7094-446b-a8a9-b995e638471a
```

Contoh berikut menunjukkan cara mendapatkan alamat MAC perangkat eth0 instans.



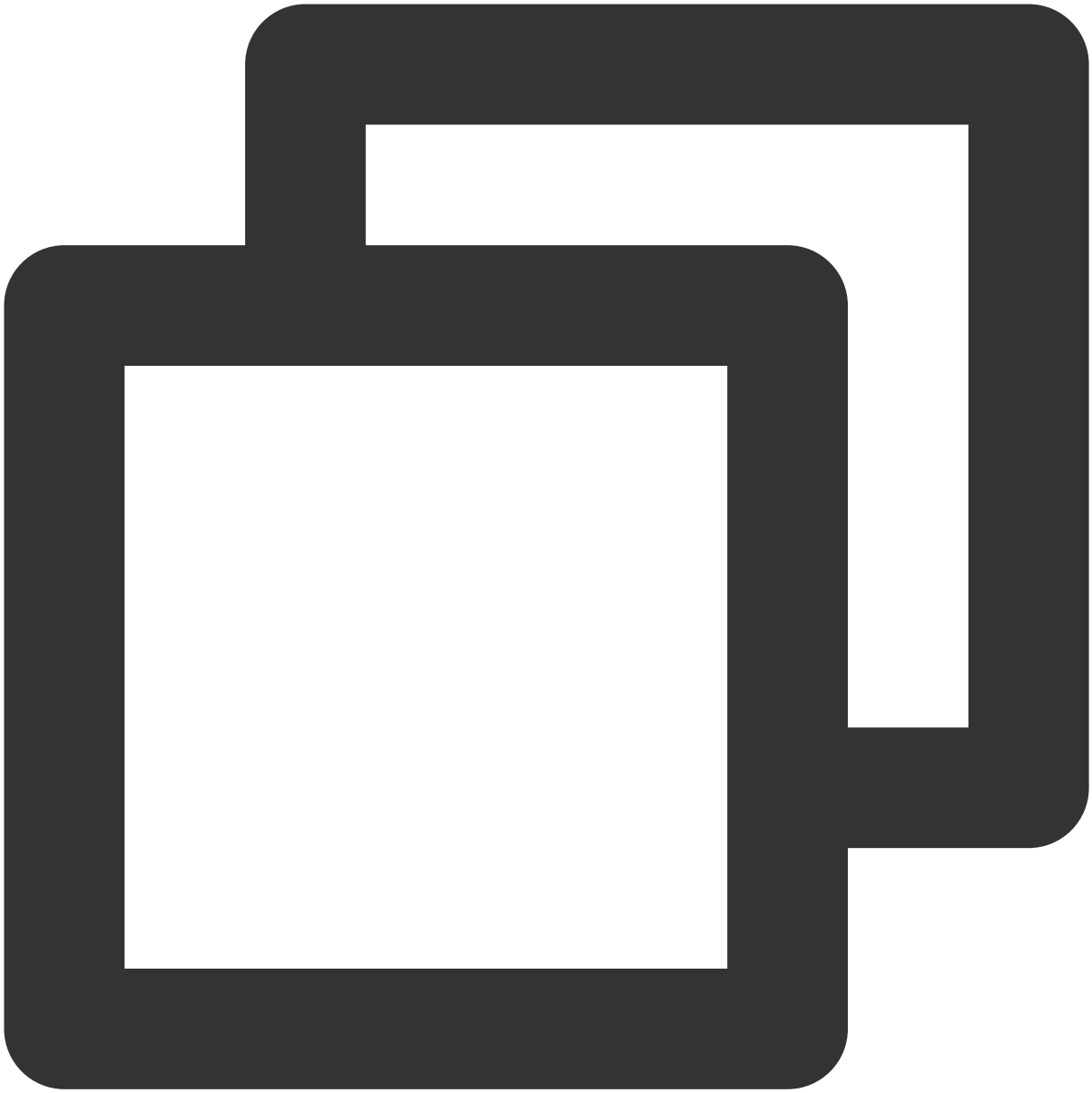
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/mac
52:54:00:BF:B3:51
```

Contoh berikut menunjukkan cara mendapatkan informasi ENI instans. Dalam kasus beberapa ENI, beberapa baris data ditampilkan, dengan setiap baris menunjukkan direktori data dari ENI.



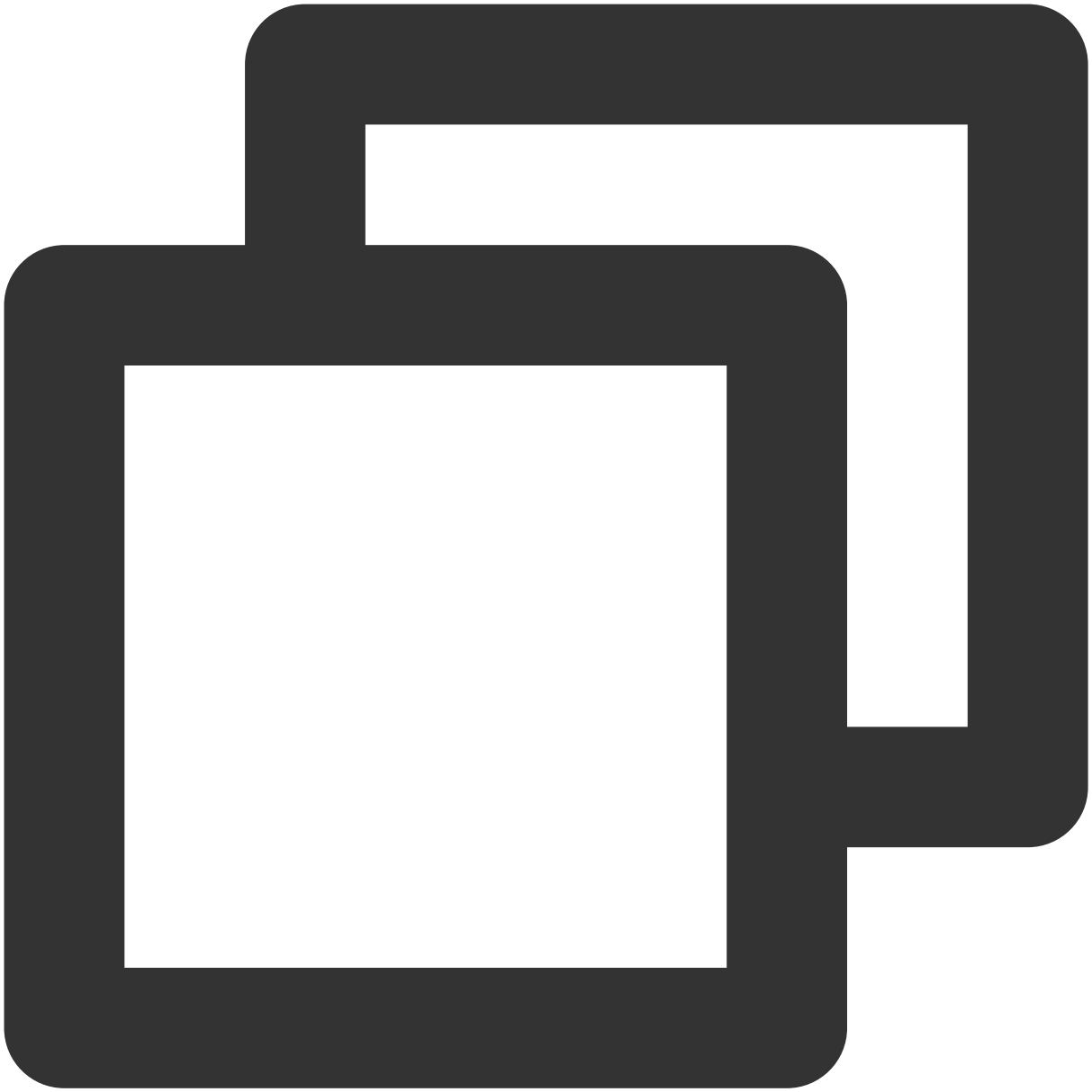
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
52:54:00:BF:B3:51/
```

Contoh berikut menunjukkan cara mendapatkan informasi dari ENI tertentu.



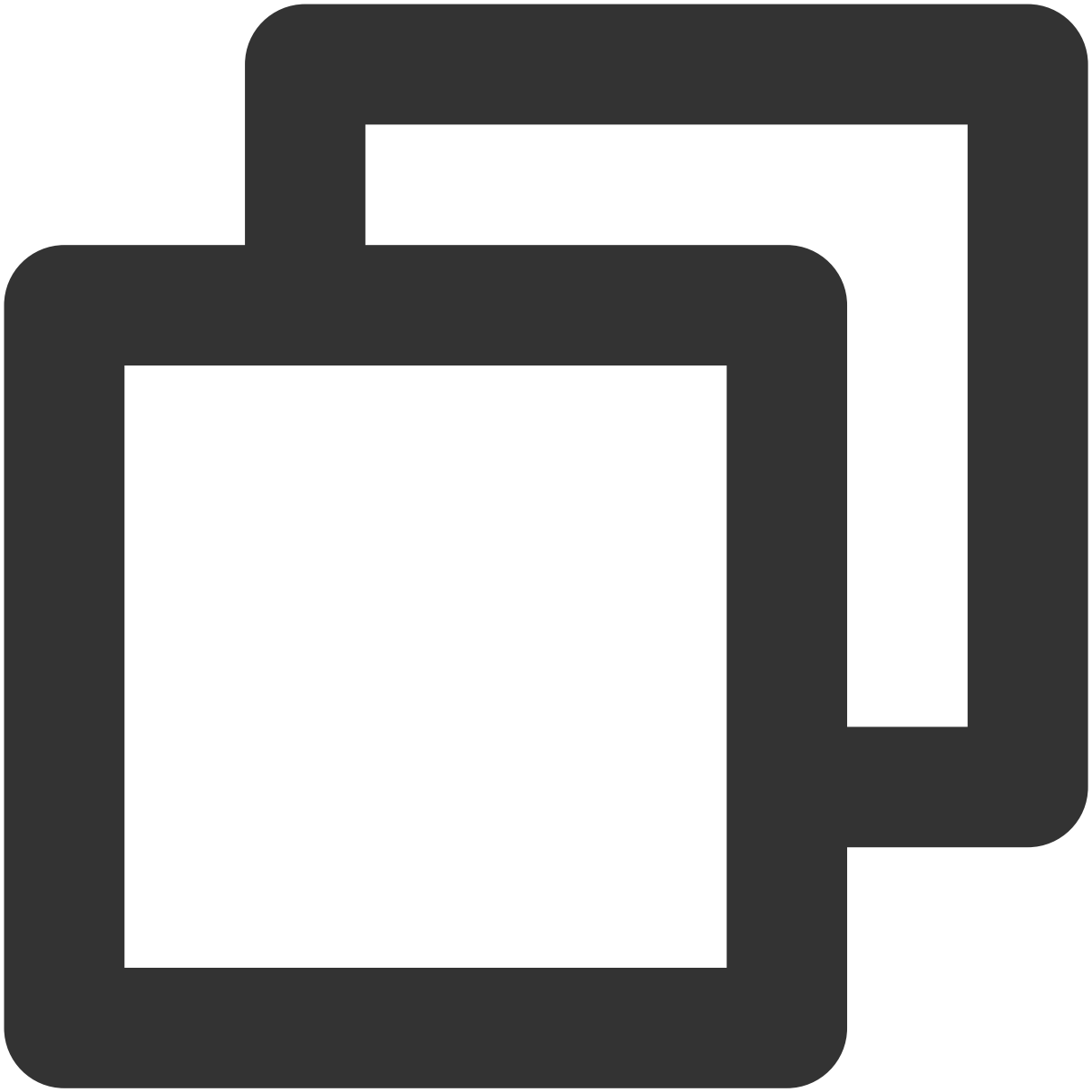
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
local-ipv4s/
mac
vpc-id
subnet-id
owner-id
primary-local-ipv4
public-ipv4s
local-ipv4s/
```

Contoh berikut menunjukkan cara mendapatkan informasi VPC dari ENI tertentu.



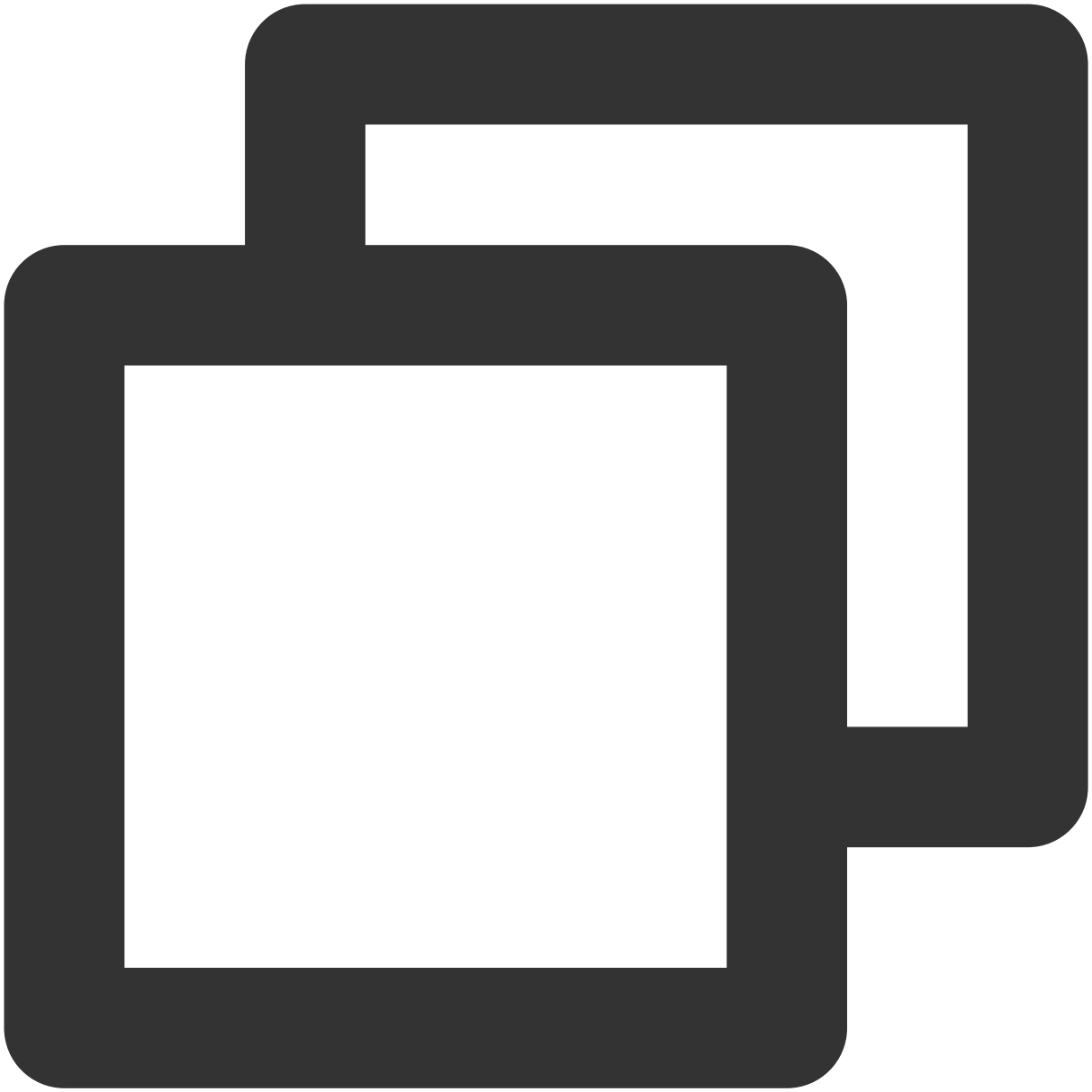
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
vpc-ja82n9op

[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
subnet-ja82n9op
```

Contoh berikut menunjukkan cara mendapatkan daftar alamat IP pribadi yang terikat ke ENI yang ditentukan. Jika ENI terikat dengan beberapa alamat IP pribadi, beberapa baris data akan ditampilkan.



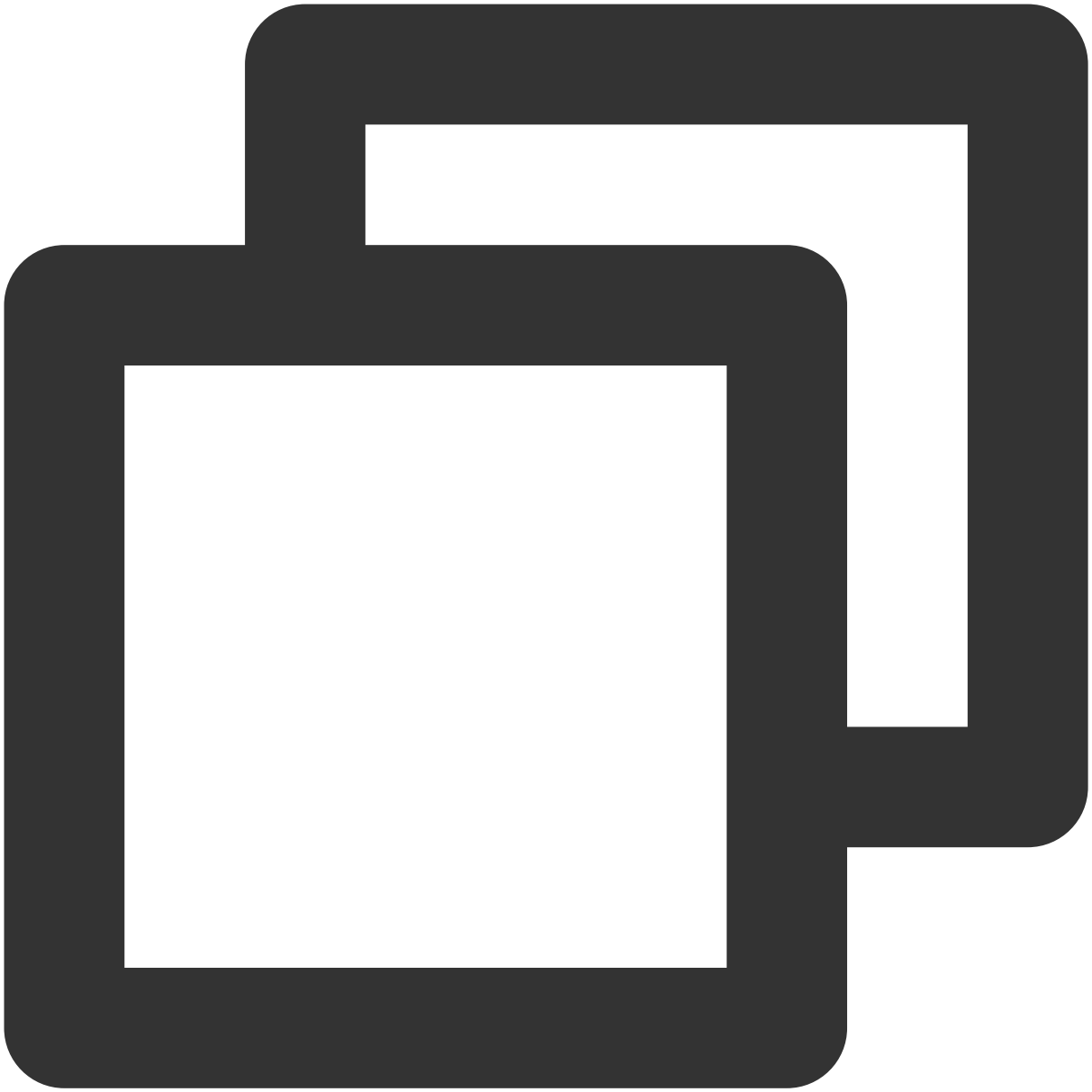
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
10.104.13.59/
```

Contoh berikut menunjukkan cara mendapatkan informasi alamat IP pribadi.



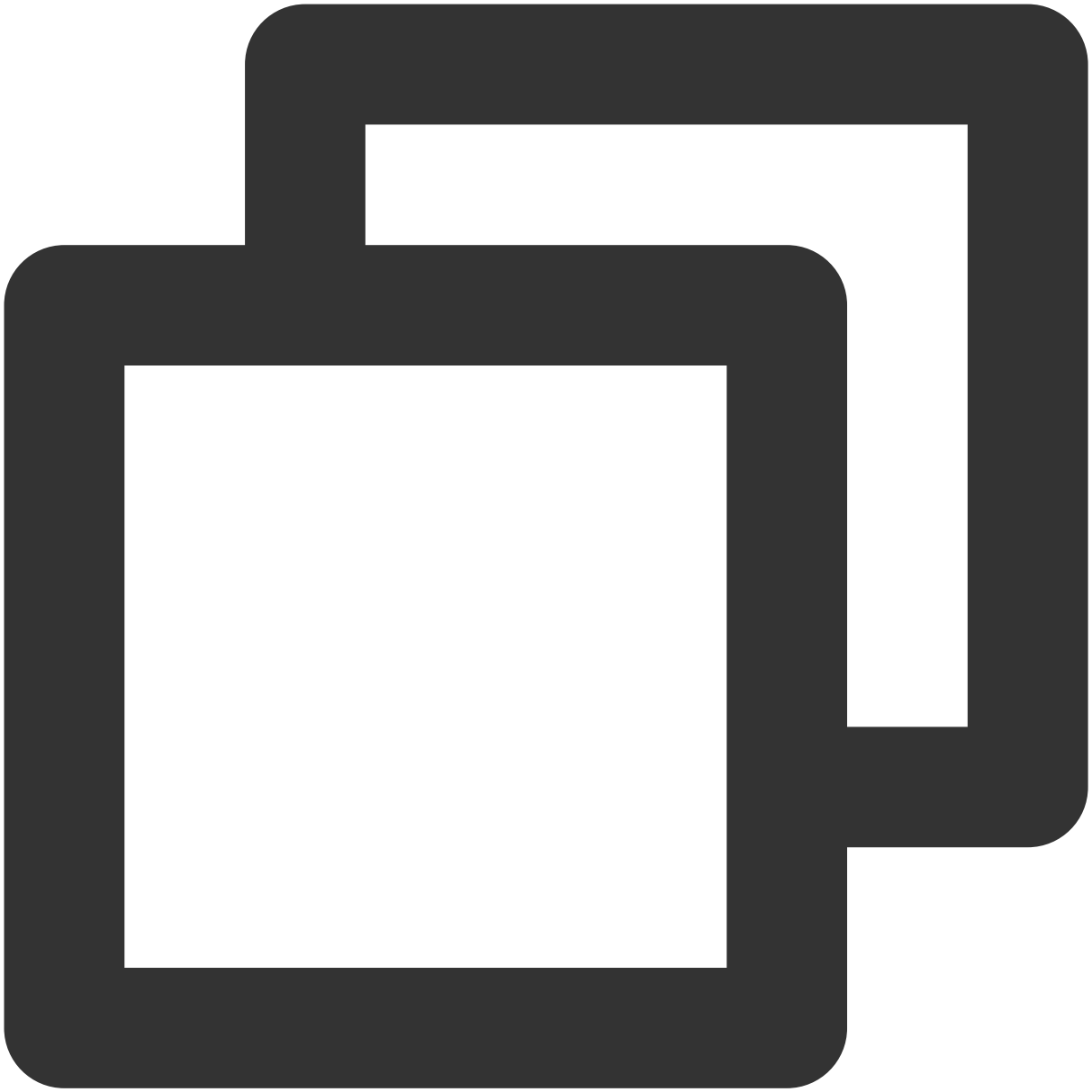
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
gateway
local-ipv4
public-ipv4
public-ipv4-mode
subnet-mask
```

Contoh berikut menunjukkan cara mendapatkan gateway alamat IP pribadi. Data ini hanya tersedia untuk model CVM berbasis VPC. Untuk informasi selengkapnya, harap lihat Virtual Private Cloud (VPC).



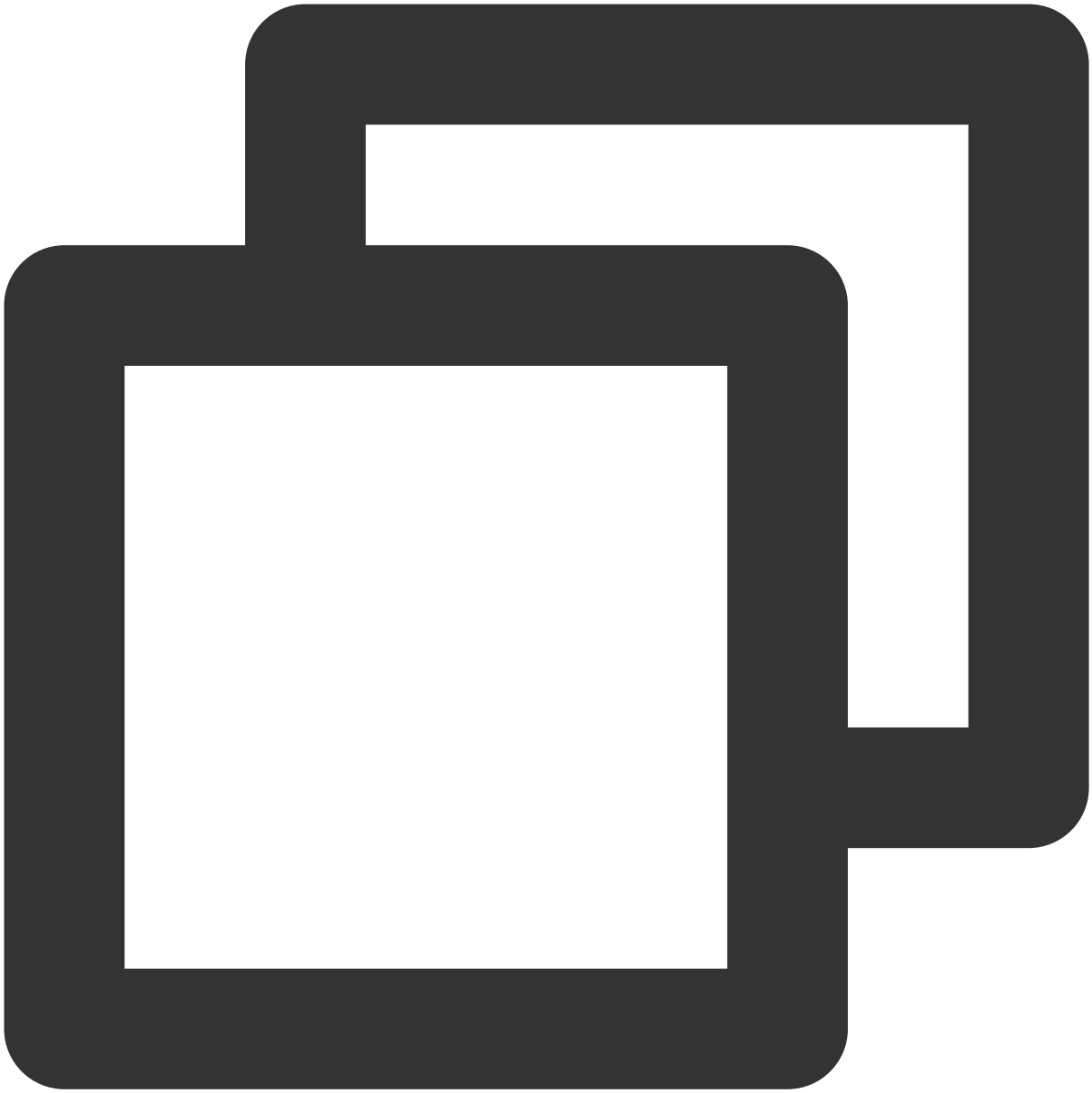
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
10.15.1.1
```

Contoh berikut menunjukkan cara mendapatkan mode akses yang digunakan oleh alamat IP pribadi untuk mengakses jaringan publik. Data ini hanya dapat dikueri untuk CVM berbasis VPC. CVM berbasis jaringan klasik mengakses jaringan publik melalui gateway publik.



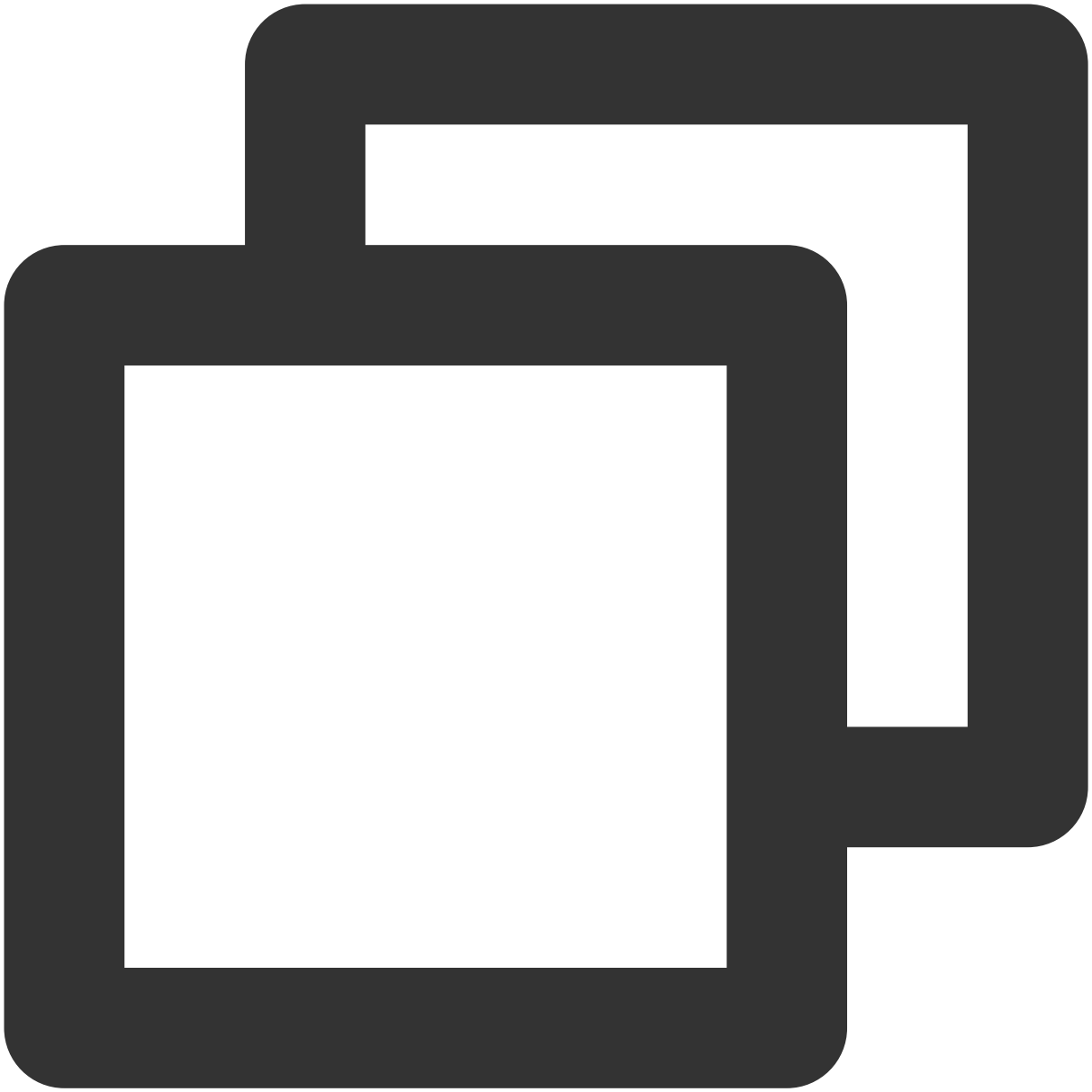
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
NAT
```

Contoh berikut menunjukkan cara mendapatkan alamat IP publik yang terikat ke alamat IP pribadi.



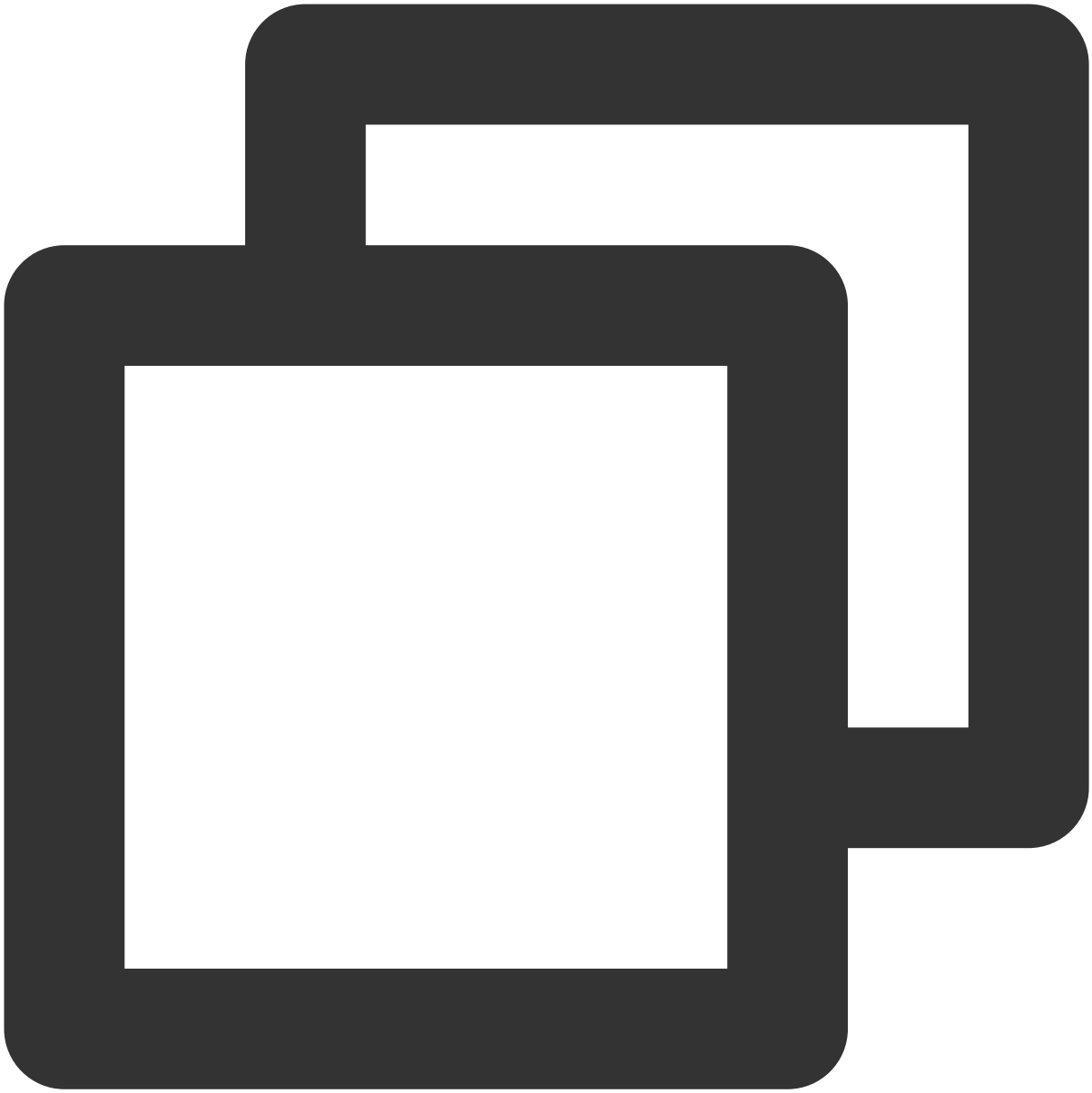
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
139.199.11.29
```

Contoh berikut menunjukkan cara mendapatkan subnet mask dari alamat IP pribadi.



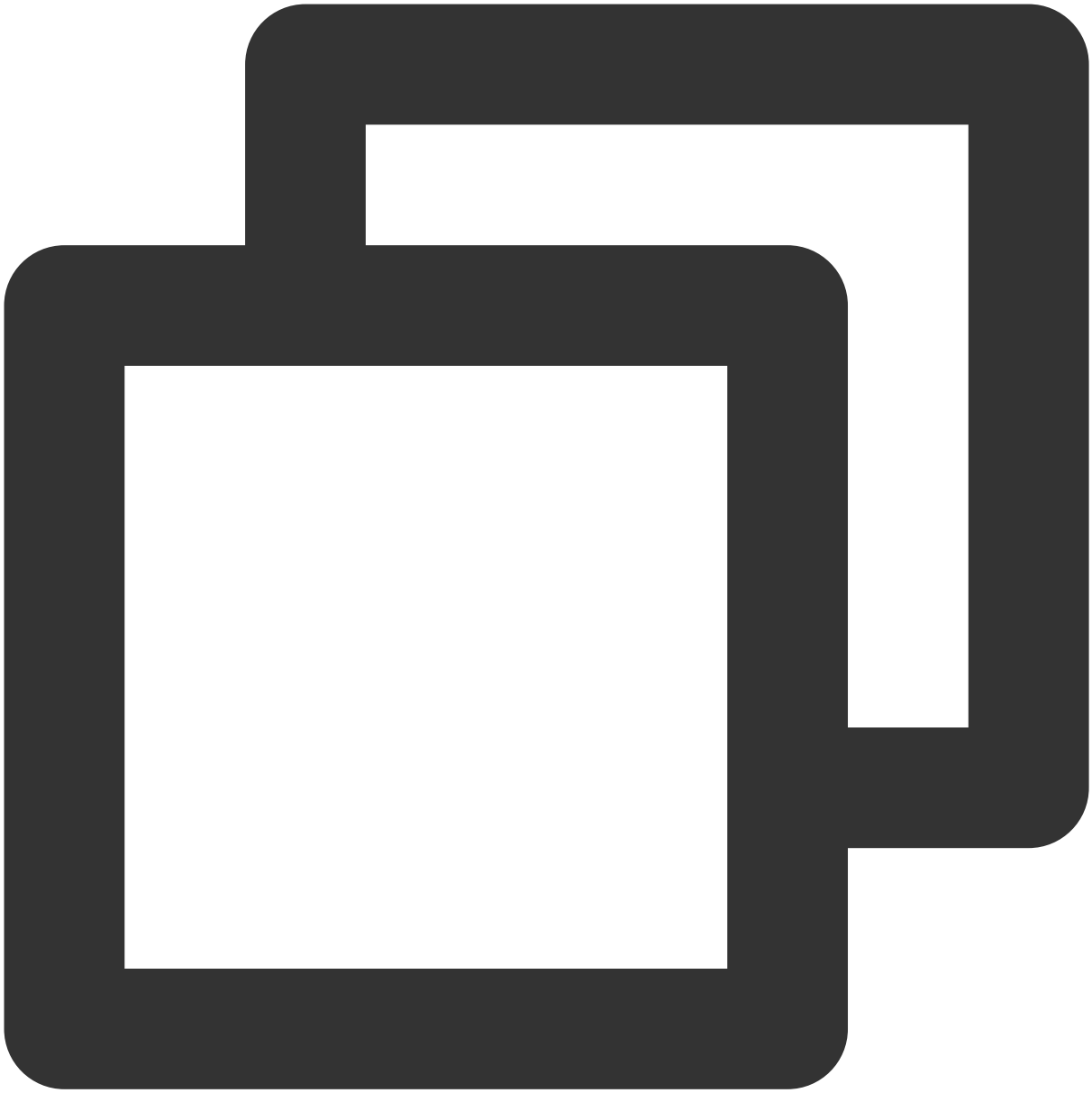
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
255.255.192.0
```

Contoh berikut menunjukkan cara mendapatkan jenis penagihan instans.



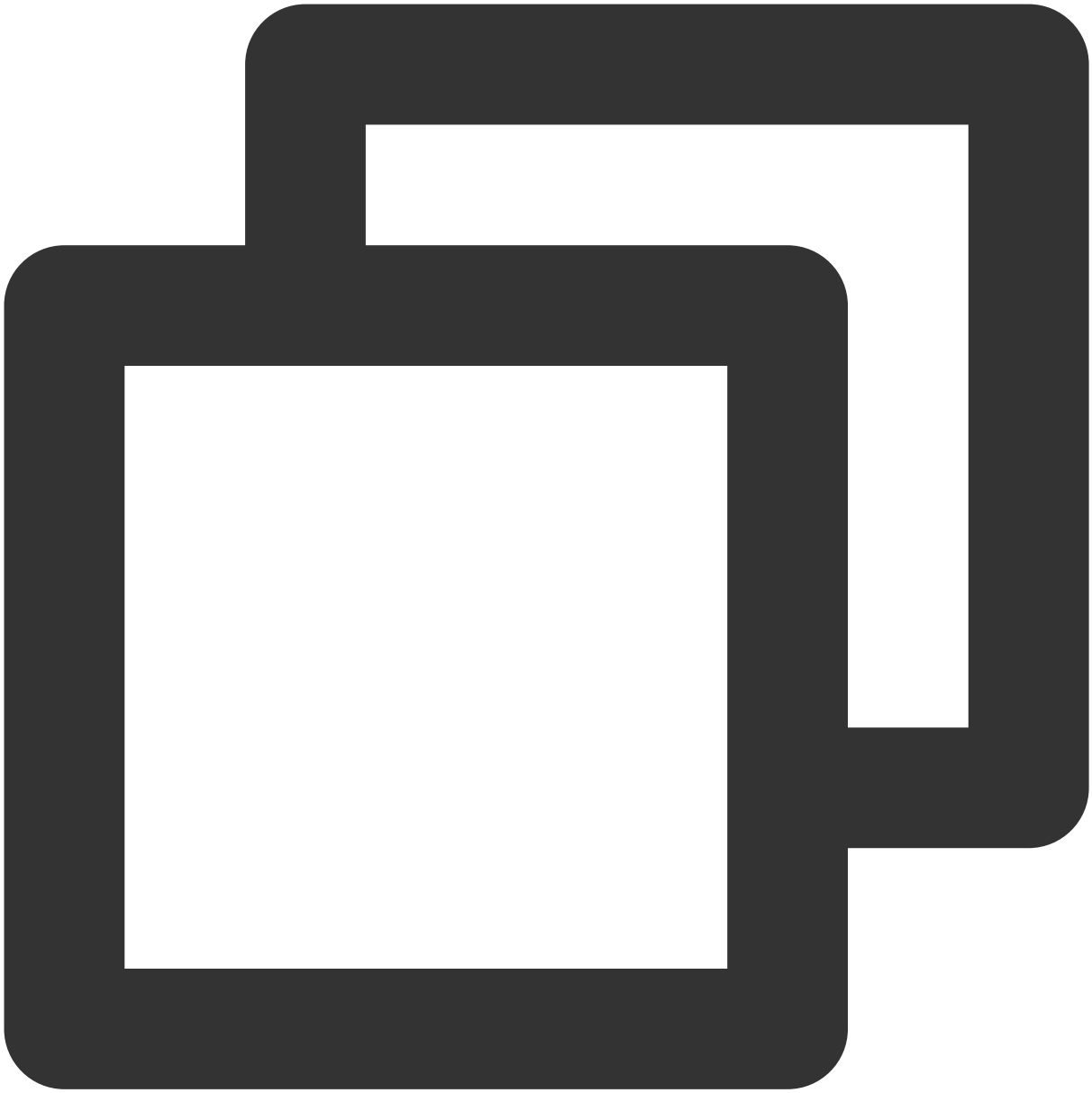
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/charge-
POSTPAID_BY_HOUR
```

Contoh berikut menunjukkan cara mendapatkan waktu pembuatan instans.



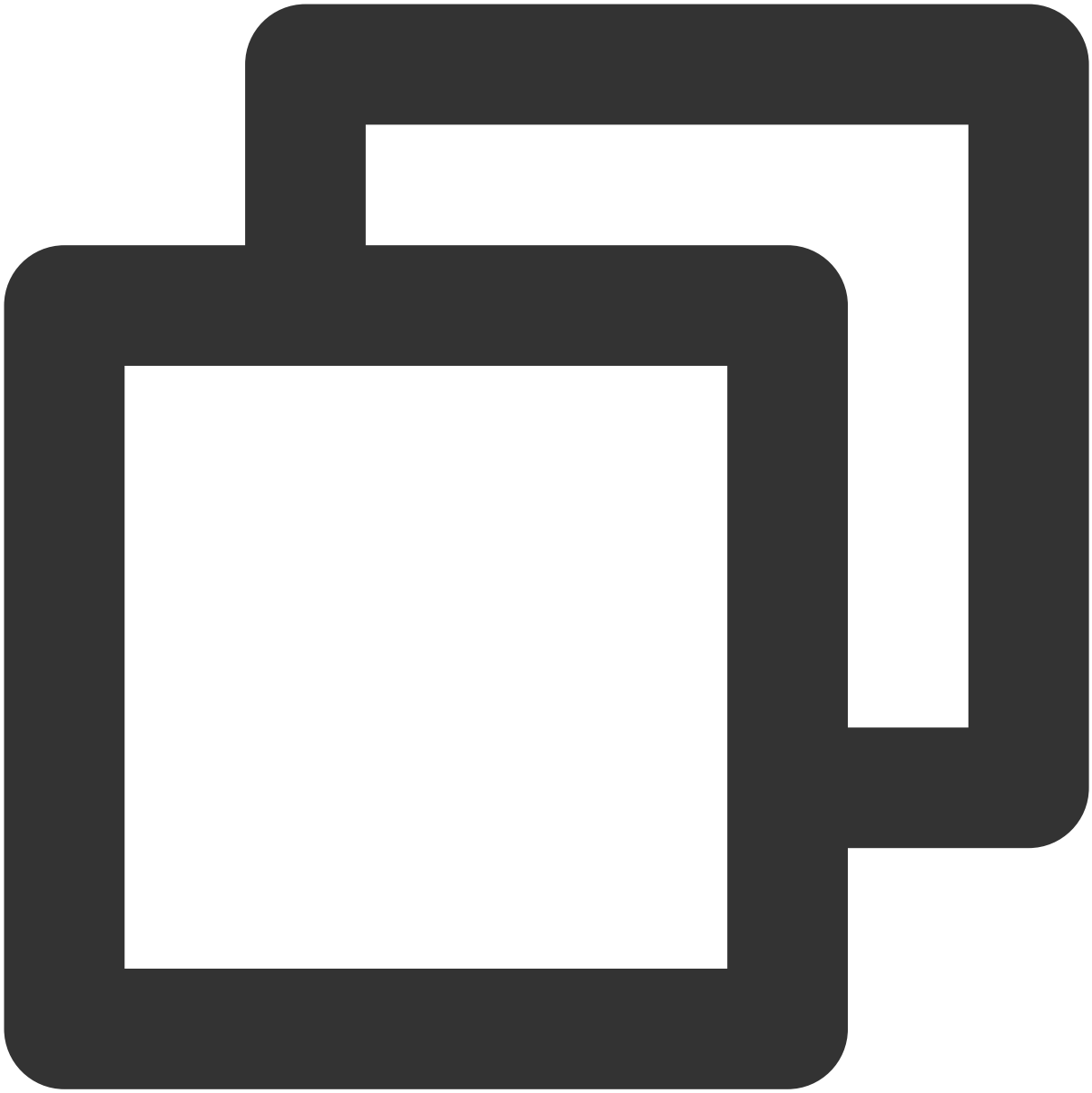
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/create-
2018-09-18 11:27:33
```

Contoh berikut menunjukkan cara mendapatkan waktu penghentian untuk instans spot.



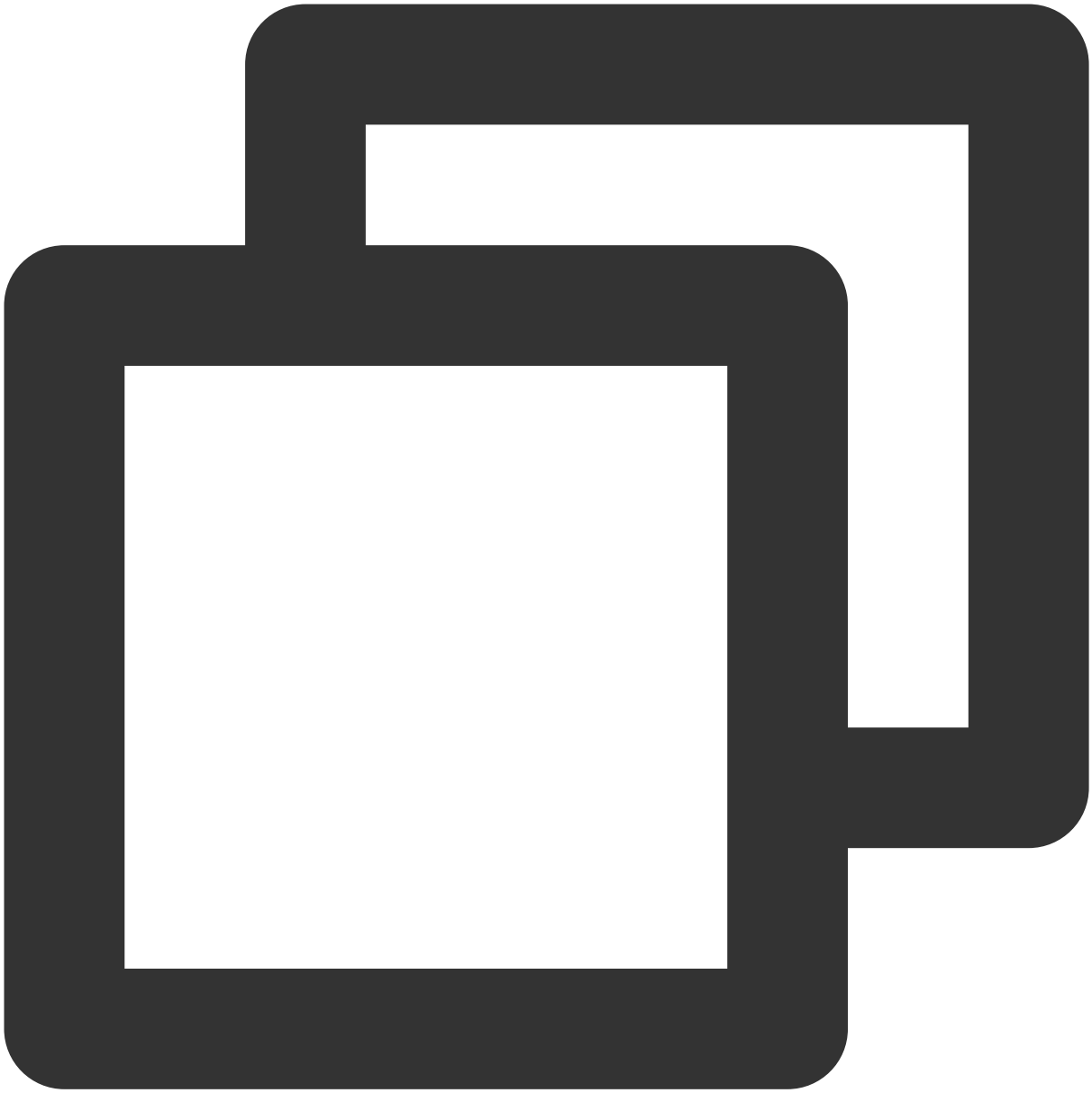
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/spot/terminatio
2018-08-18 12:05:33
```

Contoh berikut menunjukkan cara mendapatkan AppId akun tempat CVM berada.



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/app-id
123456789
```

Contoh berikut menunjukkan cara mendapatkan kredensial sementara yang dihasilkan oleh peran CAM yang menjadi milik instans. Dalam contoh ini, nama peran adalah `CVMas` .



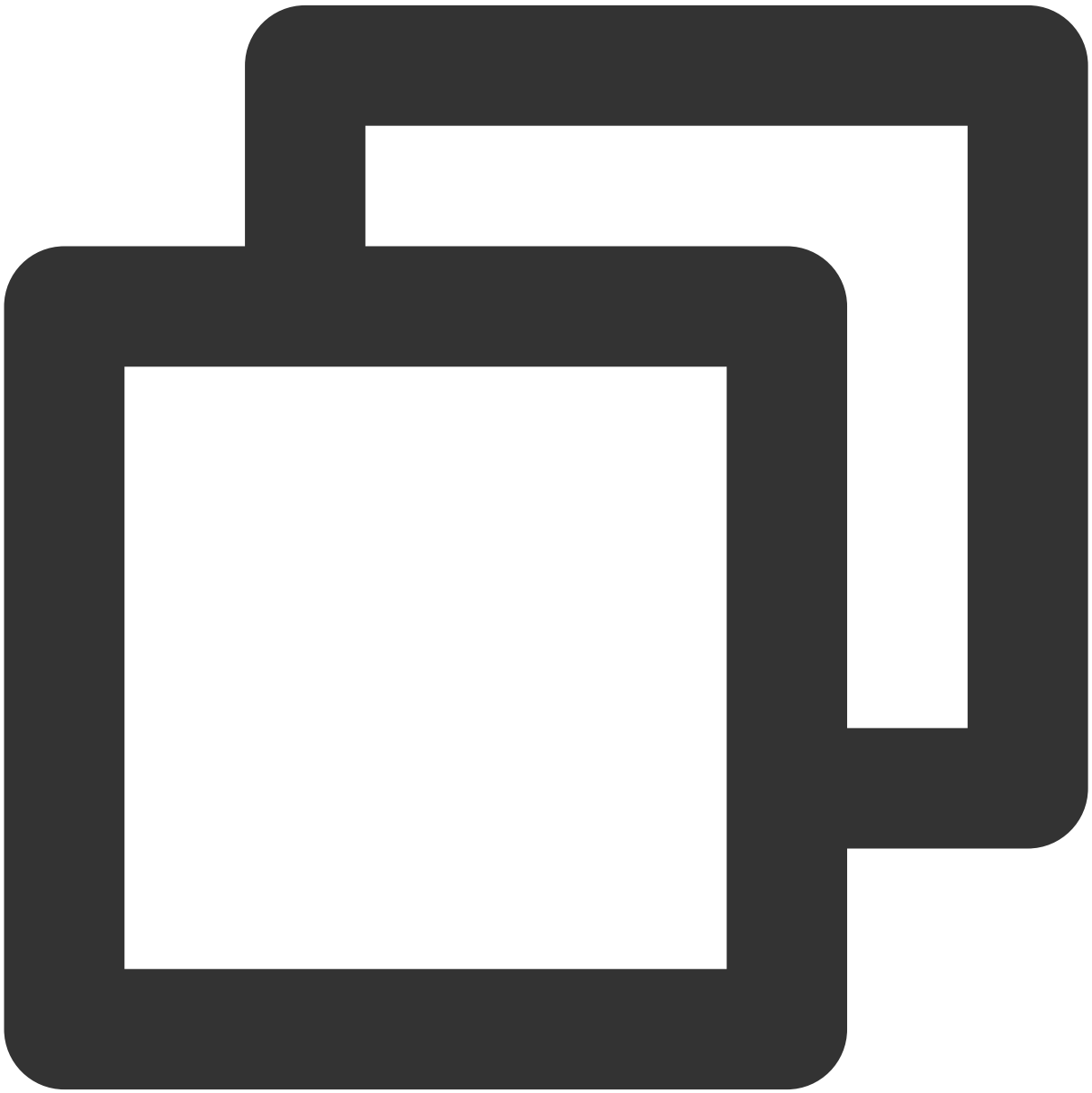
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/cam/security-cr
{
  "TmpSecretId": "AKIDoQMxF8OPg0gA7pyZIA6cW447p225cIt9NW8dhA1dwl5UvxxxxxxxxxUqRlEb5
  "TmpSecretKey": "Q9z24VucjF4xQQNV64qwF6uWY71PEsH3exxxxxxxxxgA=",
  "ExpiredTime": 1615590047,
  "Expiration": "2021-03-12T23:00:47Z",
  "Token": "xxxxxxxxxxx",
  "Code": "Success"
}
```

# Mengkueri Data Pengguna Instans

Anda dapat menentukan data pengguna instans saat membuat instans. Instans CVM yang memiliki konfigurasi cloud-init dapat mengakses data.

### Mencari data pengguna

Setelah login, Anda dapat mengakses data pengguna dengan menggunakan metode berikut.



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/user-data
179, klien, shanghai
```

# Mengganti Nama Instans

Waktu update terbaru：2021-12-13 17:07:04

## Skenario

Untuk membantu pengguna mengelola instans CVM di konsol dan menemukan CVM dengan cepat berdasarkan nama, Tencent Cloud memungkinkan pengguna mengganti nama instans kapan saja dan nama baru akan langsung berlaku.

## Petunjuk

### Memodifikasi nama instans

1. Login ke Konsol CVM.
2. Dalam daftar instans, pilih CVM yang namanya perlu diubah dan klik **More**(Lainnya) > **Instance Settings**(Pengaturan Instans) > **Rename** (Ganti nama) di sebelah kanan.
3. Di jendela “Rename” (Ganti nama) yang muncul, masukkan nama instans baru, lalu klik **OK** (OKE).

### Memodifikasi nama beberapa instans

1. Login ke Konsol CVM.
2. Dalam daftar instans, pilih beberapa instans CVM yang namanya perlu diubah, lalu klik **More actions**(Tindakan lainnya)>**Instance Settings**(Pengaturan Instans) > **Rename** (Ganti Nama) di bagian atas.
3. Di jendela “Rename” (Ganti nama) yang muncul, masukkan nama instans baru, lalu klik **OK** (OKE).

**Keterangan:**
CVM yang dimodifikasi dengan menggunakan metode ini akan memiliki nama instans yang sama.

# Mengatur Ulang Kata Sandi Instans

Waktu update terbaru：2021-12-13 17:07:04

## Ikhtisar

Jika lupa kata sandi login instans CVM, harap atur ulang kata sandi tersebut di konsol.

**Perhatian:**

Anda dapat langsung mengatur ulang kata sandi login dari instans pematian.

Mengatur ulang kata sandi login dari instans yang sedang berjalan akan memaksanya dimatikan. Untuk menghindari kehilangan data, harap rencanakan sebelumnya dan atur ulang kata sandi selama jam tidak sibuk.

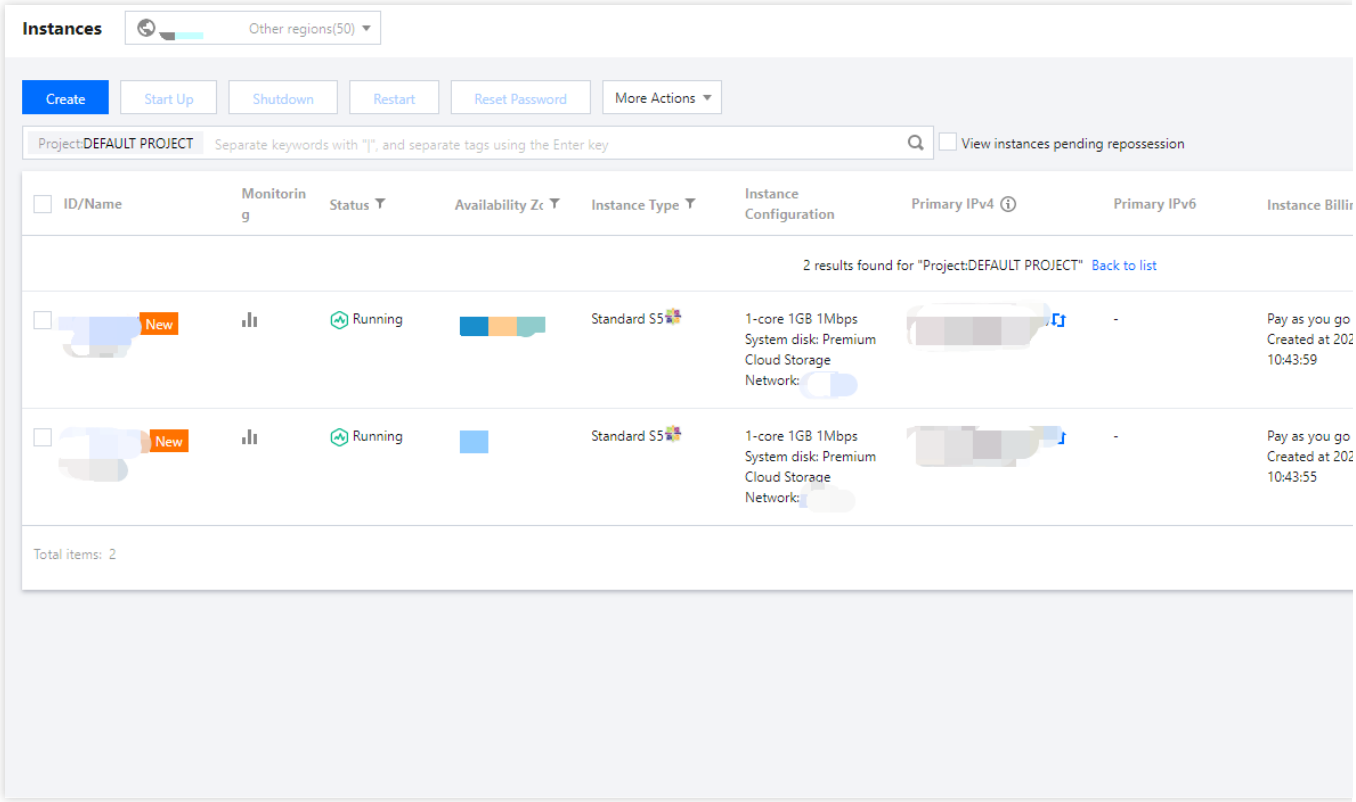
## Petunjuk

Resetting the password of a single instance

Resetting the passwords of multiple instances

1. Login ke konsol CVM.

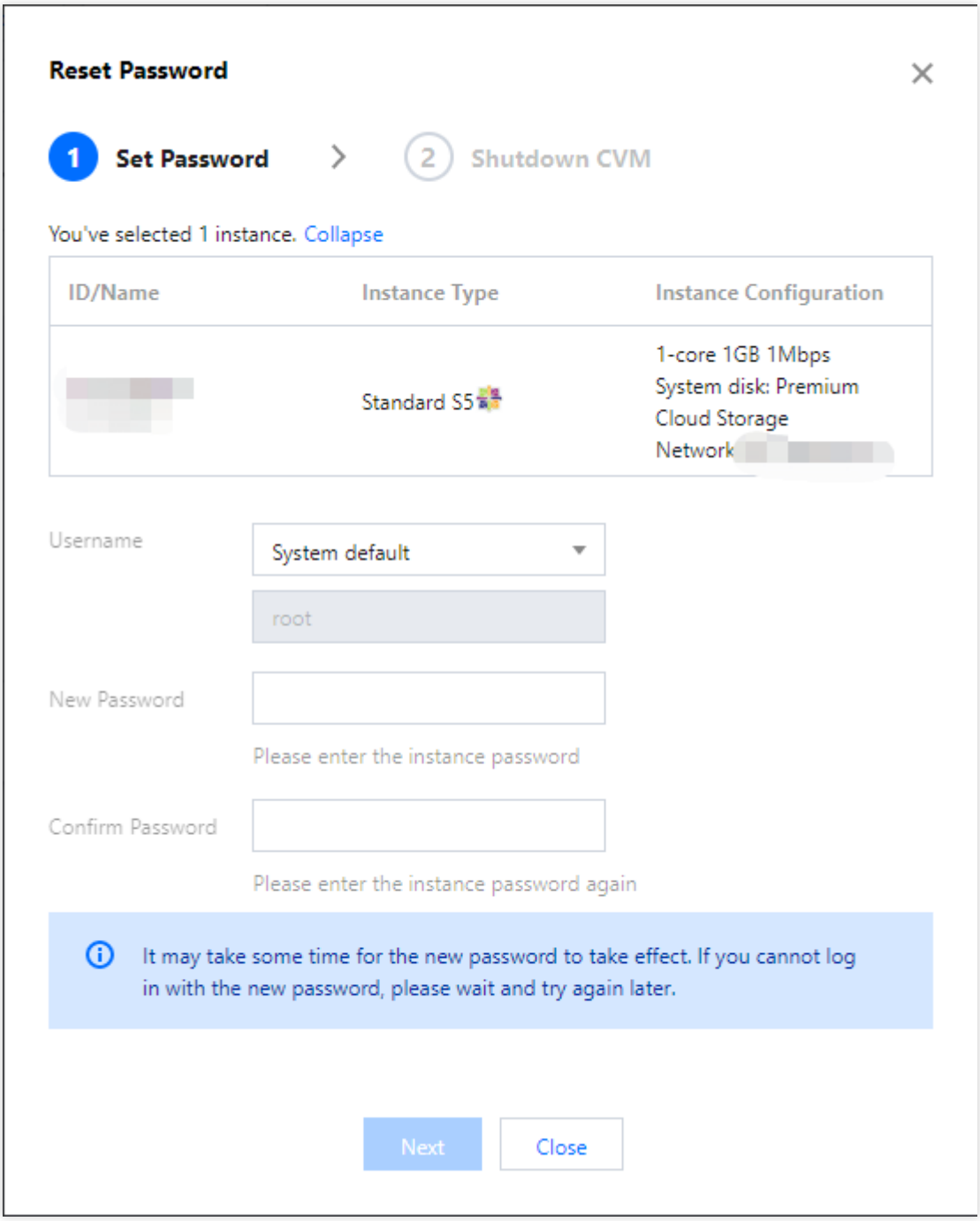
2. Pada halaman **Instances** (Instans), cari instans CVM target, lalu klik **More** (Lainnya) > **Password/Key** (Kata Sandi/Kunci) > **Reset Password** (Atur Ulang Kata Sandi) di kolom **Operation** (Operasi), seperti yang ditunjukkan pada gambar berikut:




3. Pilih **Username** (Nama Pengguna) dan masukkan nama pengguna dari instans yang dipilih. Masukkan **New password** (Kata sandi baru), masukkan kembali kata sandi baru di kolom **Confirm Password** (Konfirmasi Kata Sandi), lalu klik **Next** (Berikutnya).

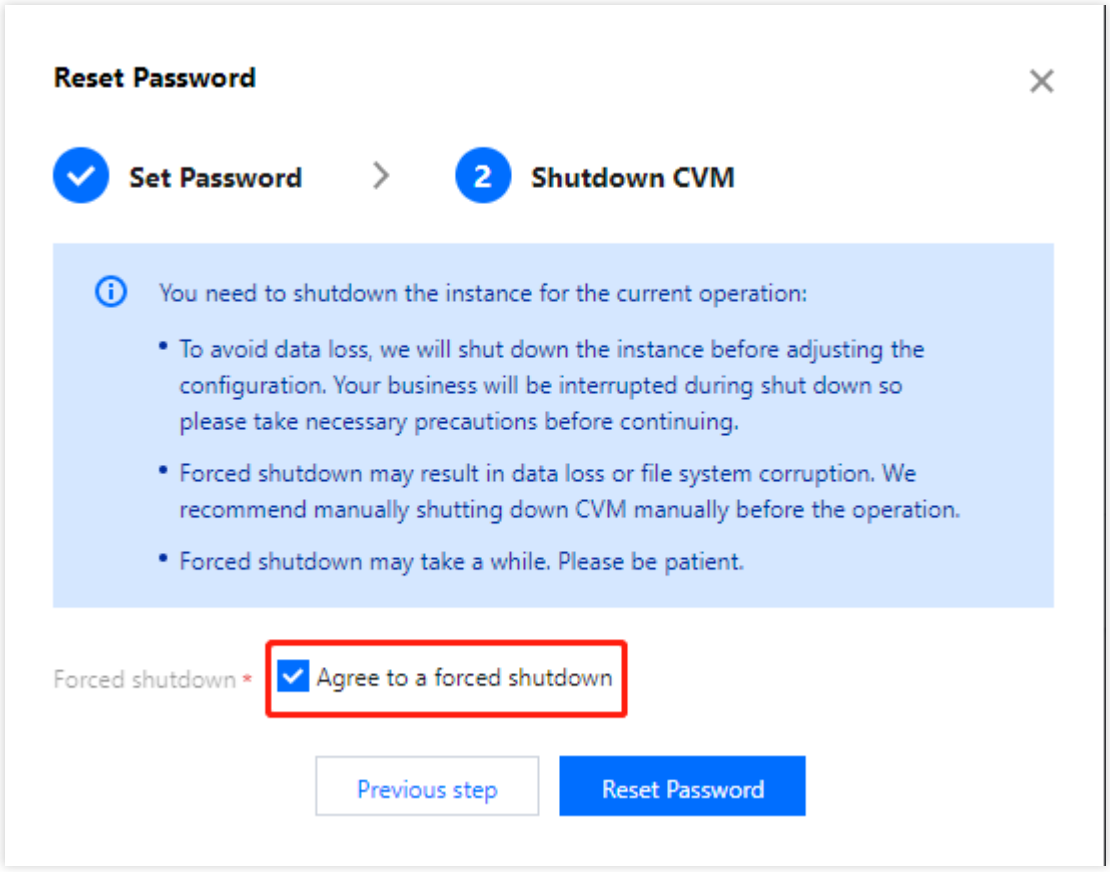
**Perhatian:**

**Username** (Nama Pengguna) defaultnya adalah **System default** (Default sistem), dan nama pengguna sistem default digunakan, seperti “Administrator” untuk Windows, “ubuntu” untuk Ubuntu, dan “root” untuk distribusi Linux lainnya. Anda dapat memilih **Specified user name** (Nama pengguna yang ditentukan) dan memasukkan nama pengguna.

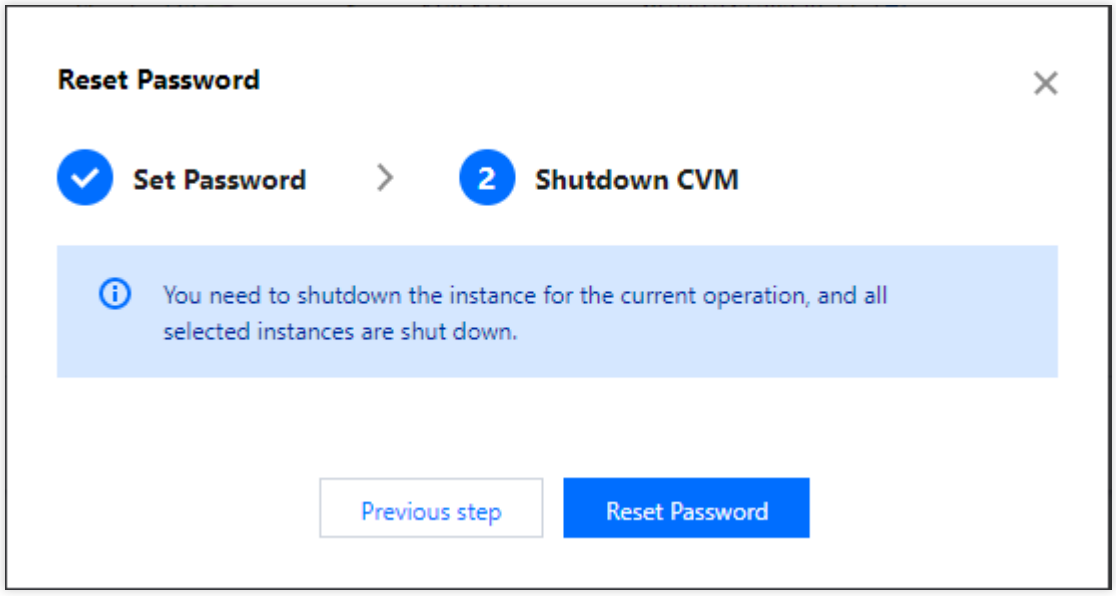



4. Atur ulang kata sandi sesuai dengan status instans:

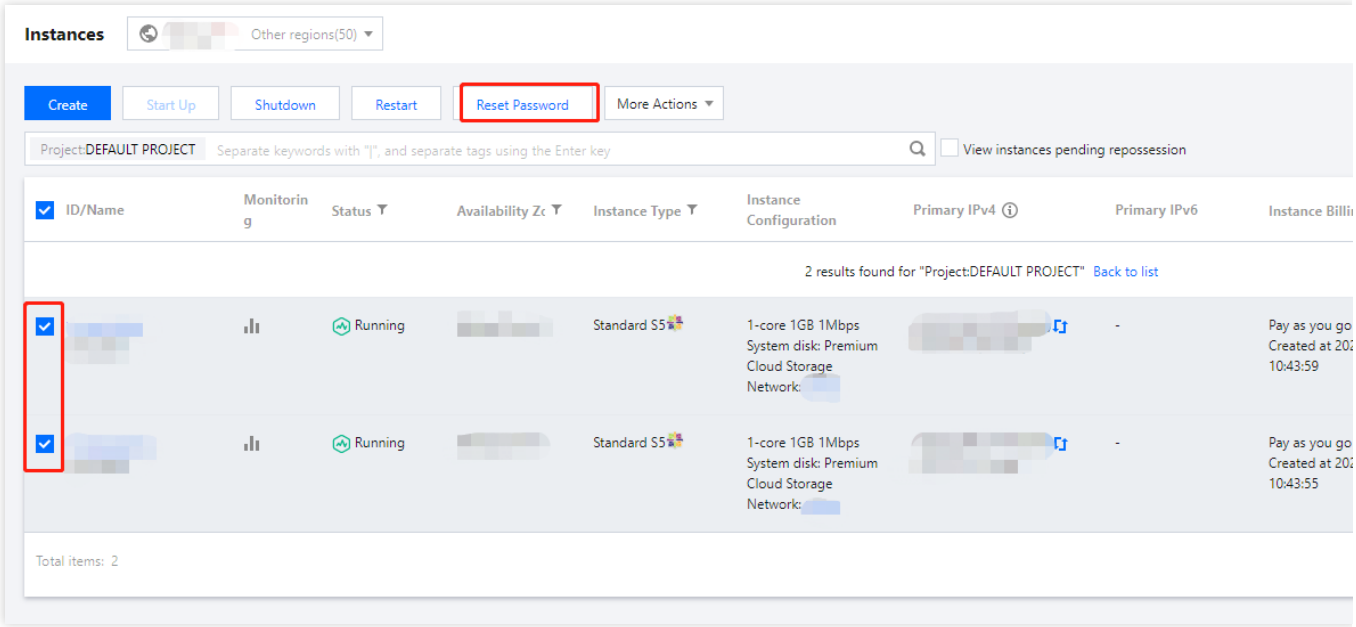
Untuk mengatur ulang kata sandi instans yang **Running** (Berjalan), pilih **Agree to force shutdown** (Setujui pematian paksa), lalu klik **Reset Password** (Atur Ulang Kata Sandi), seperti yang ditunjukkan pada gambar berikut:




Untuk mengatur ulang kata sandi instans yang **Shutdown** (Dimatikan), klik **Reset Password** (Atur Ulang Kata Sandi), seperti yang ditunjukkan pada gambar berikut.



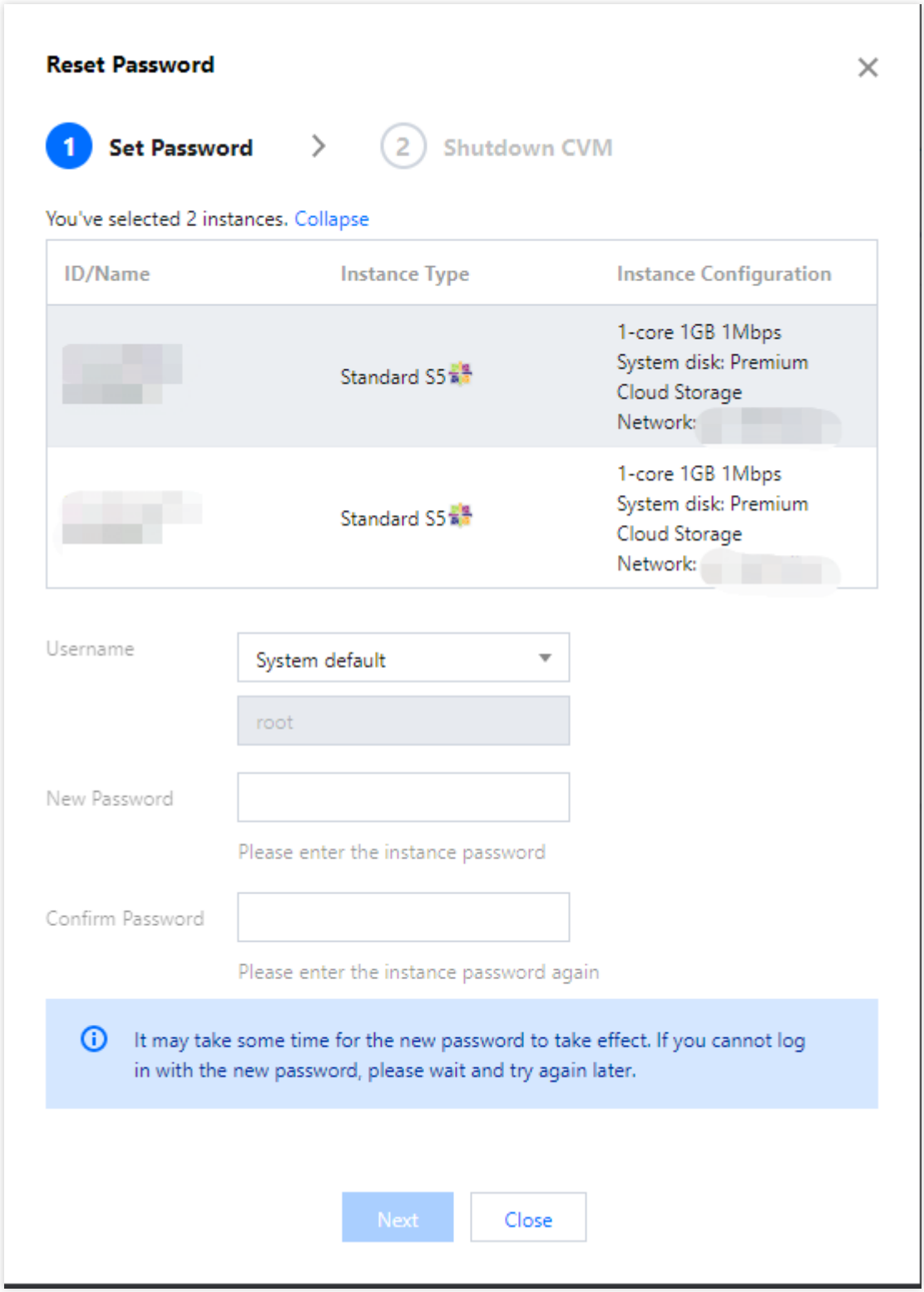

1. Login ke konsol CVM.
2. Pada halaman **Instances** (Instans), pilih instans CVM untuk mengatur ulang kata sandi, lalu klik **Reset Password** (Atur Ulang Kata Sandi) di bagian atas daftar instans, seperti yang ditunjukkan pada gambar berikut:




3. Pilih **Username** (Nama Pengguna) dan masukkan nama pengguna dari instans yang dipilih. Masukkan **New password** (Kata sandi baru), masukkan kembali kata sandi baru di kolom **Confirm Password** (Konfirmasi Kata Sandi), lalu klik **Next** (Berikutnya).

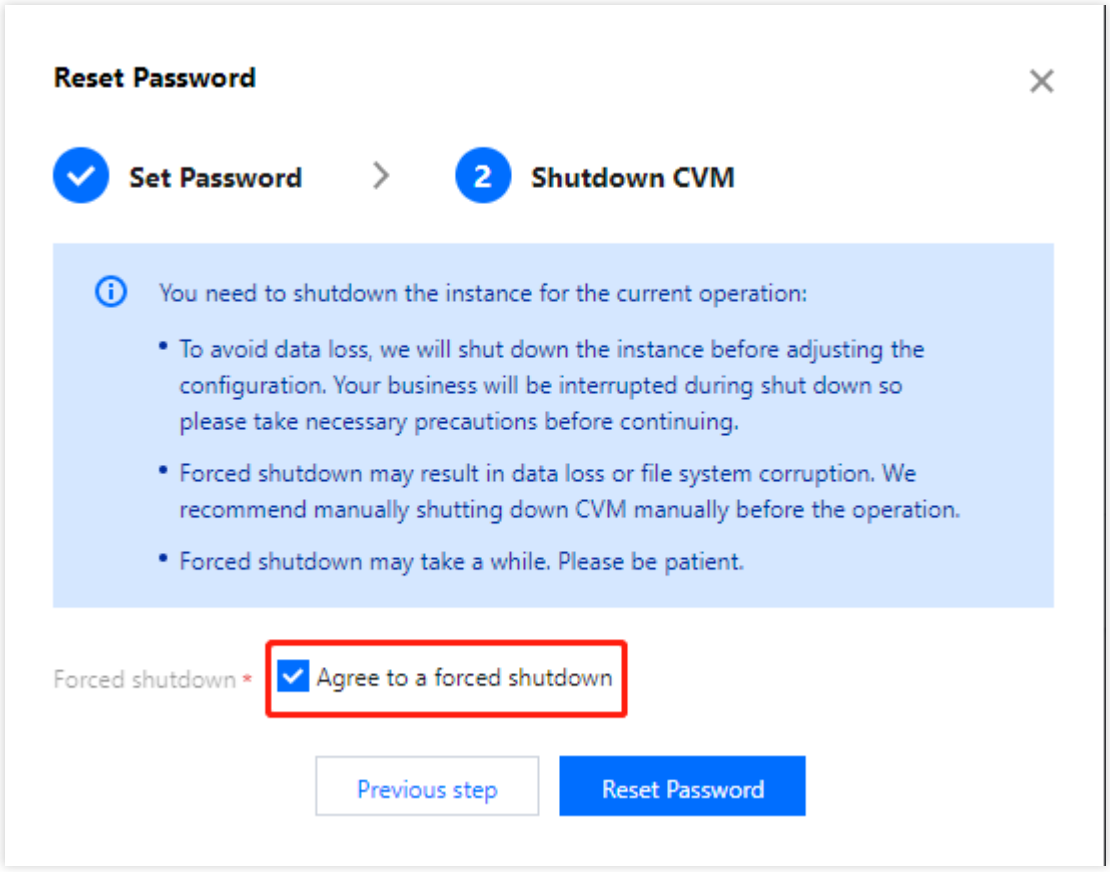
**Perhatian:**

**Username** (Nama Pengguna) defaultnya adalah **System default** (Default sistem), dan nama pengguna sistem default digunakan, seperti “Administrator” untuk Windows, “ubuntu” untuk Ubuntu, dan “root” untuk distribusi Linux lainnya. Anda dapat memilih **Specified user name** (Nama pengguna yang ditentukan) dan memasukkan nama pengguna.

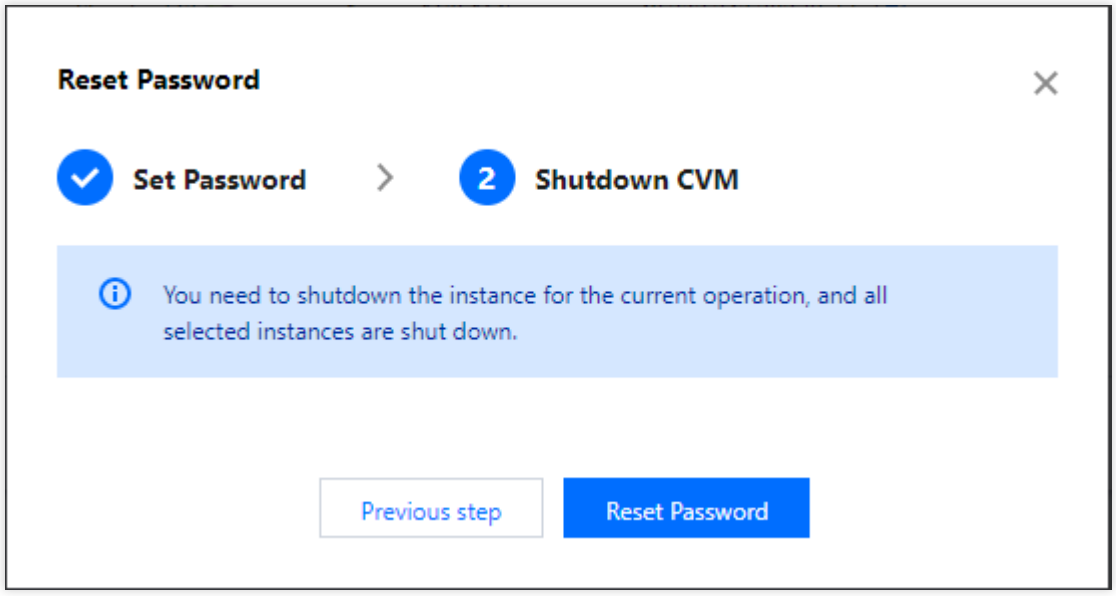



4. Atur ulang kata sandi sesuai dengan status instans:

Untuk mengatur ulang kata sandi instans yang **Running** (Berjalan), pilih **Agree to force shutdown** (Setujui pematian paksa), lalu klik **Reset Password** (Atur Ulang Kata Sandi), seperti yang ditunjukkan pada gambar berikut:




Untuk mengatur ulang kata sandi instans yang **Shutdown** (Dimatikan), klik **Reset Password** (Atur Ulang Kata Sandi), seperti yang ditunjukkan pada gambar berikut.



# Alamat IP instans manajemen
# Mendapatkan Alamat IP Pribadi dan Mengatur DNS

Waktu update terbaru：2022-07-08 15:51:40

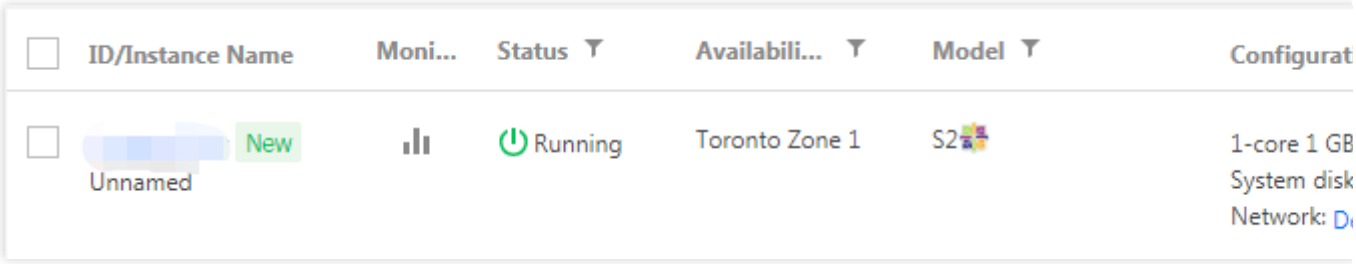
Dokumen ini menjelaskan cara mendapatkan alamat IP pribadi dari instans dan mengonfigurasi DNS pribadi.

## Mendapatkan alamat IP pribadi dari instans

### Mendapatkan alamat IP pribadi di konsol

1. Login ke Konsol CVM.
2. Pada halaman manajemen instans, pilih instans dan gerakkan mouse ke kolom **Primary IP** (IP Primer) untuk melihat IP pribadinya, dan klik

untuk menyalin IP pribadi, seperti yang ditunjukkan di bawah ini:




### Mendapatkan alamat IP pribadi menggunakan API

Harap Lihat DescribeInstances API.

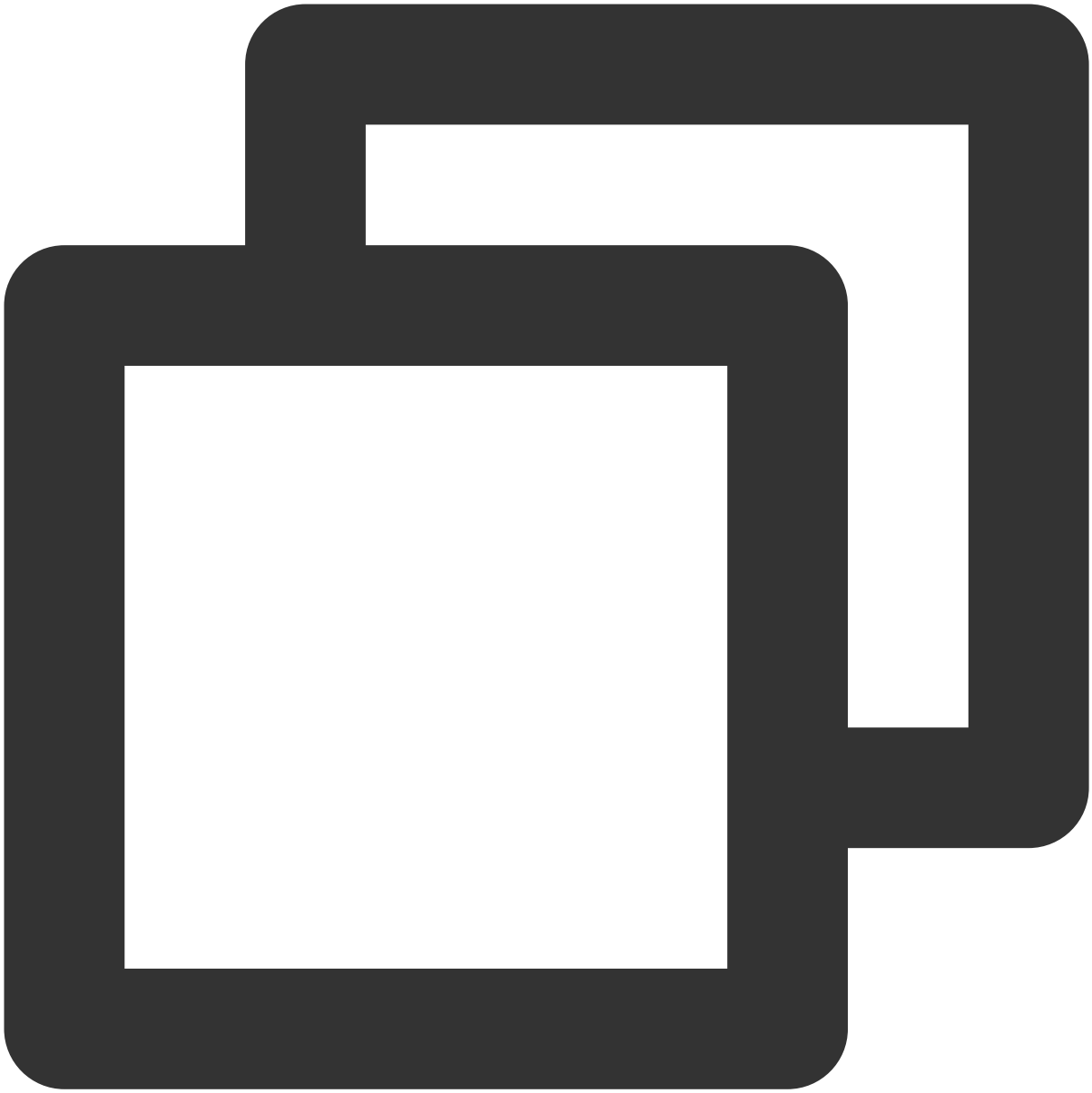
### Mendapatkan alamat IP pribadi menggunakan metadata instans

1. Login ke CVM.
2. Akses metadata instans dengan menggunakan alat cURL atau permintaan HTTP GET.

**Keterangan:**

Operasi berikut menggunakan alat cURL sebagai contoh.

Jalankan perintah berikut untuk mendapatkan IP pribadi.



```
curl http://metadata.tencentyun.com/meta-data/local-ipv4
```

Informasi yang dikembalikan adalah alamat IP pribadi, seperti yang ditunjukkan di bawah ini:

```
[root@VM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/local-ipv4
10.XXX.XX.27
```

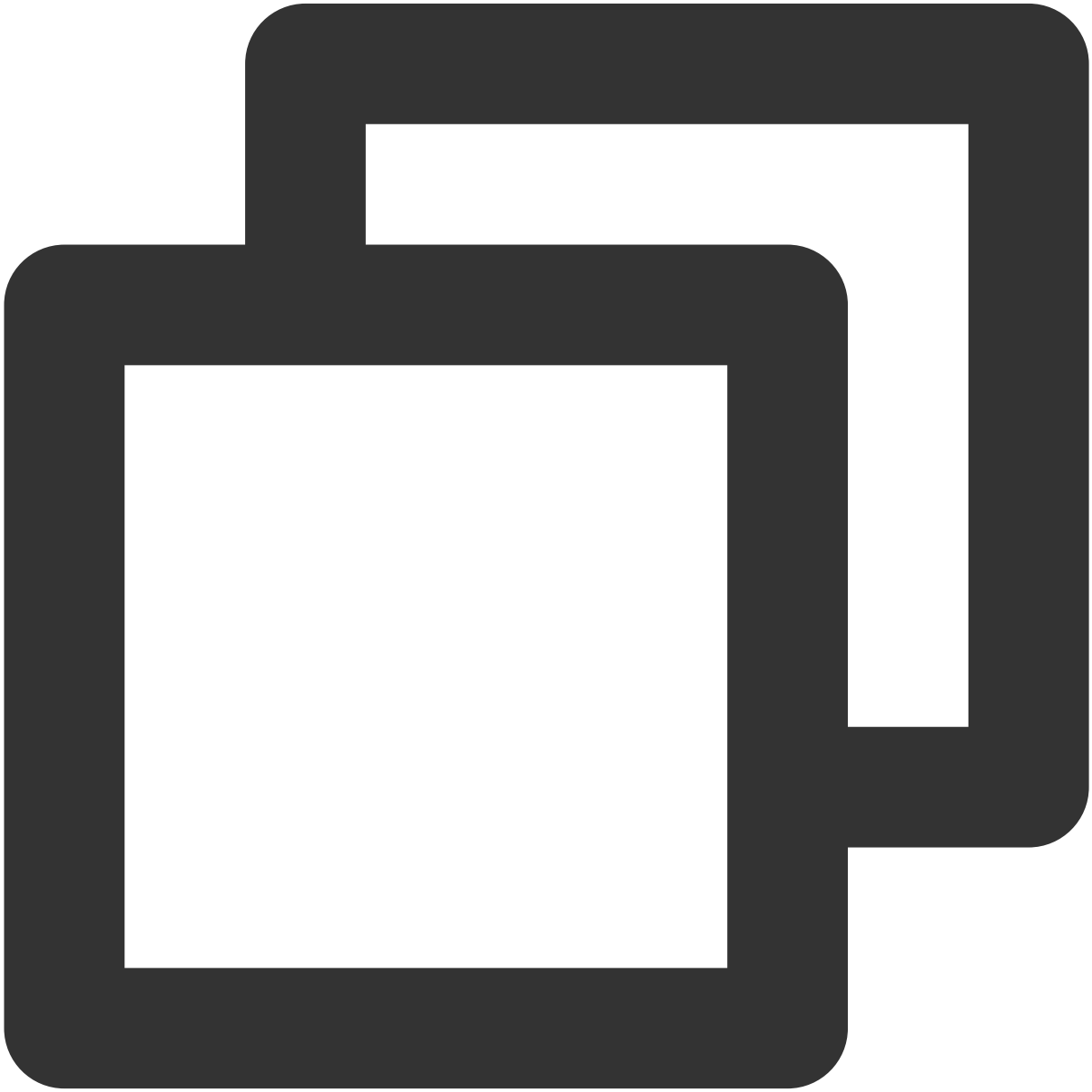
Untuk informasi selengkapnya tentang metadata instans, lihat Metadata Instans.

# Mengonfigurasi DNS jaringan pribadi

Ketika terjadi kesalahan resolusi jaringan, Anda dapat mengonfigurasi DNS jaringan pribadi secara manual berdasarkan sistem operasi CVM Anda.

## Untuk sistem operasi Linux

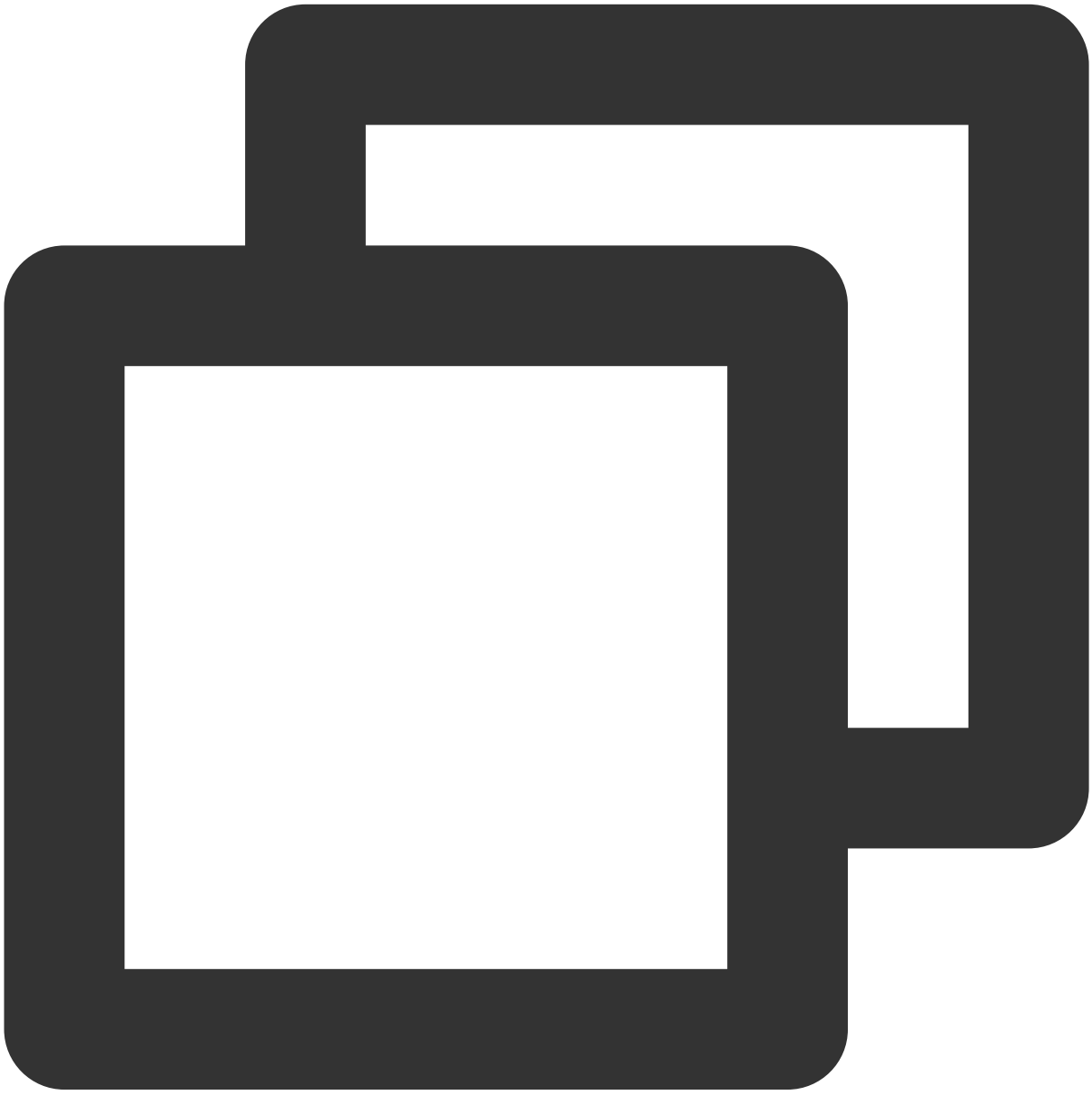
1. Login ke CVM Linux.
2. Jalankan perintah berikut untuk membuka file `/etc/resolv.conf` .



```
vi /etc/resolv.conf
```

3. Tekan **i** (i) untuk beralih ke mode edit, dan ubah IP DNS sesuai dengan wilayah terkait dalam daftar DNS Jaringan Pribadi.

Misalnya, untuk mengubah IP DNS jaringan pribadi menjadi server DNS jaringan pribadi di wilayah Beijing.

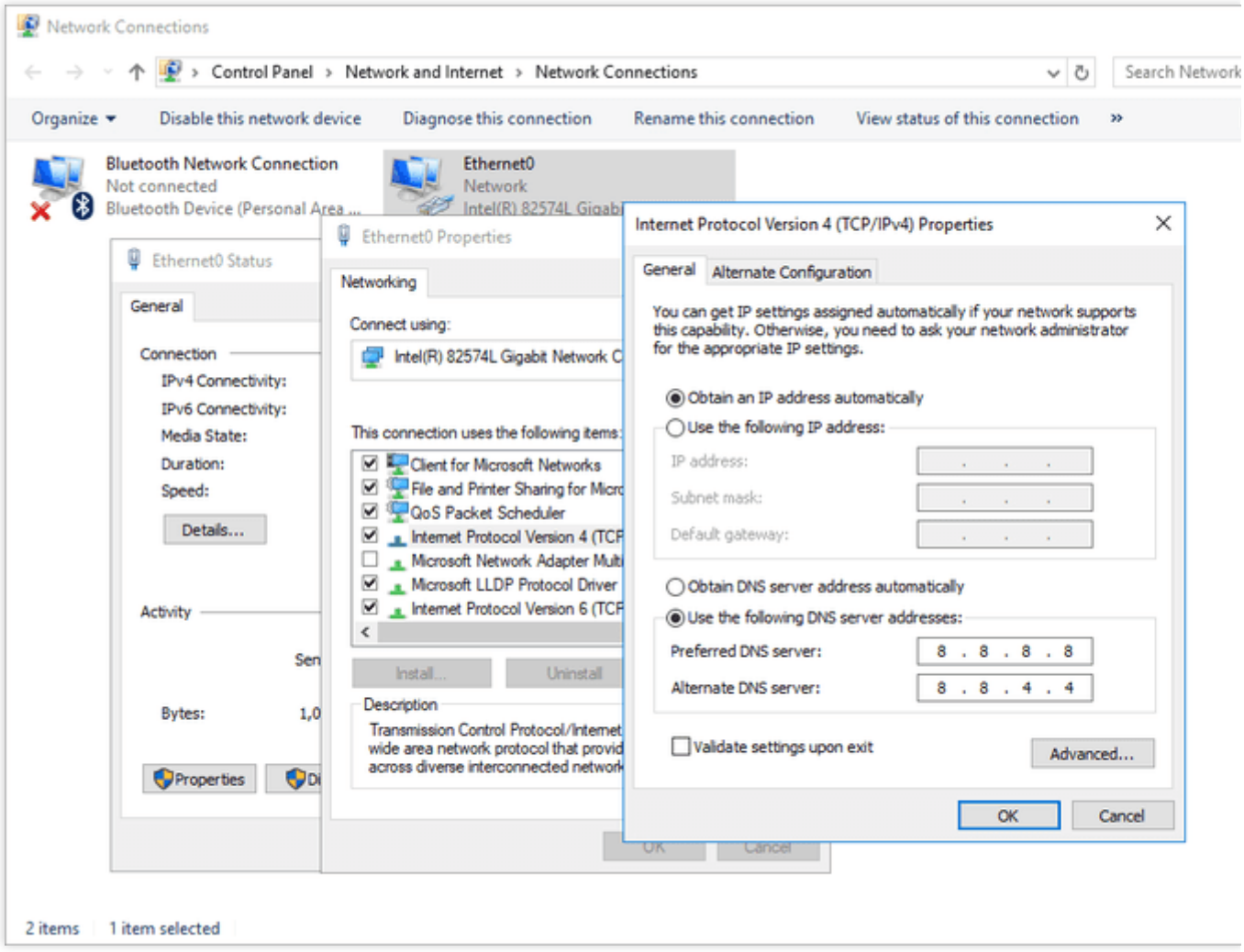


```
server nama 10.53.216.182
server nama 10.53.216.198
batas waktu opsi: 1 putar
```

4. Tekan **Esc** (Esc), masukkan **:wq** (:wq), simpan file dan kembalikan.

### Untuk sistem operasi Windows

1. Login ke CVM Windows.
2. Pada antarmuka sistem operasi, buka **Control Panel** (Panel Kontrol) > **Network and Sharing Center** (Pusat Jaringan dan Berbagi) > **Change adapter settings** (Ubah pengaturan adaptor).
3. Klik kanan **Ethernet** (Ethernet) dan pilih **Properties** (Properti) untuk membuka jendela “Ethernet Properties” (Properti Ethernet).
4. Di jendela “Ethernet Properties” (Properti Ethernet), klik dua kali **IP version 4 (TCP/IPv4)** (IP versi 4 (TCP/IPv4)), seperti yang ditunjukkan di bawah ini:




5. Pilih **Gunakan alamat server DNS berikut** dan ubah IP DNS sesuai dengan wilayah yang sesuai dalam daftar DNS Jaringan Pribadi.
6. Klik **OK** (OKE).

# Memodifikasi Alamat IP Pribadi

Waktu update terbaru：2023-04-21 15:52:30

## Skenario

Anda dapat mengubah IP pribadi instans CVM di VPC langsung di konsol atau dengan mengubah subnet instans CVM. Dokumen ini menjelaskan cara mengubah IP pribadi instans CVM di konsol VPC.
Untuk detail tentang mengubah subnet, lihat Ubah Subnet Instans.

## Batas

Memodifikasi IP primer dari ENI primer dapat menyebabkan CVM dimulai ulang.
IP primer ENI sekunder tidak dapat diubah.

## Petunjuk

1. Login ke Konsol CVM.
2. Pilih wilayah instans yang IP pribadinya yang ingin Anda ubah, dan klik ID/nama instans untuk masuk ke halaman detailnya.
3. Pada halaman detail instans, pilih tab [ENI] dan klik

untuk memperluas ENI primer.
4. Dalam daftar operasi ENI utama, klik **Modify Primary IP** (Modifikasi IP Primer).
5. Di jendela “Modify Primary IP” (Modifikasi IP Primer) yang muncul, masukkan IP baru lalu klik **OK** (OKE). Ini berlaku setelah instans dimulai ulang.

**Perhatian:**

Anda hanya dapat memasukkan IP pribadi di CIDR subnet saat ini.

# Mendapatkan Alamat IP Publik

Waktu update terbaru：2021-12-13 17:07:04

## Skenario

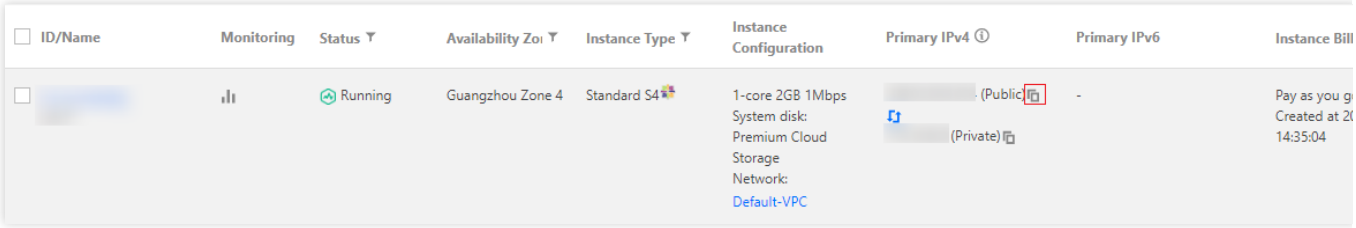
Dokumen ini menjelaskan cara mendapatkan alamat IP publik melalui konsol, API, atau metadata Instans.

## Petunjuk

### Mendapatkan alamat IP publik di konsol

1. Login ke Konsol CVM.
2. Pada halaman manajemen instans, gerakkan mouse ke kolom IP utama, dan

</ img> akan muncul, seperti yang ditunjukkan di bawah ini:




3. Klik

untuk menyalin alamat IP.

**Perhatian:**

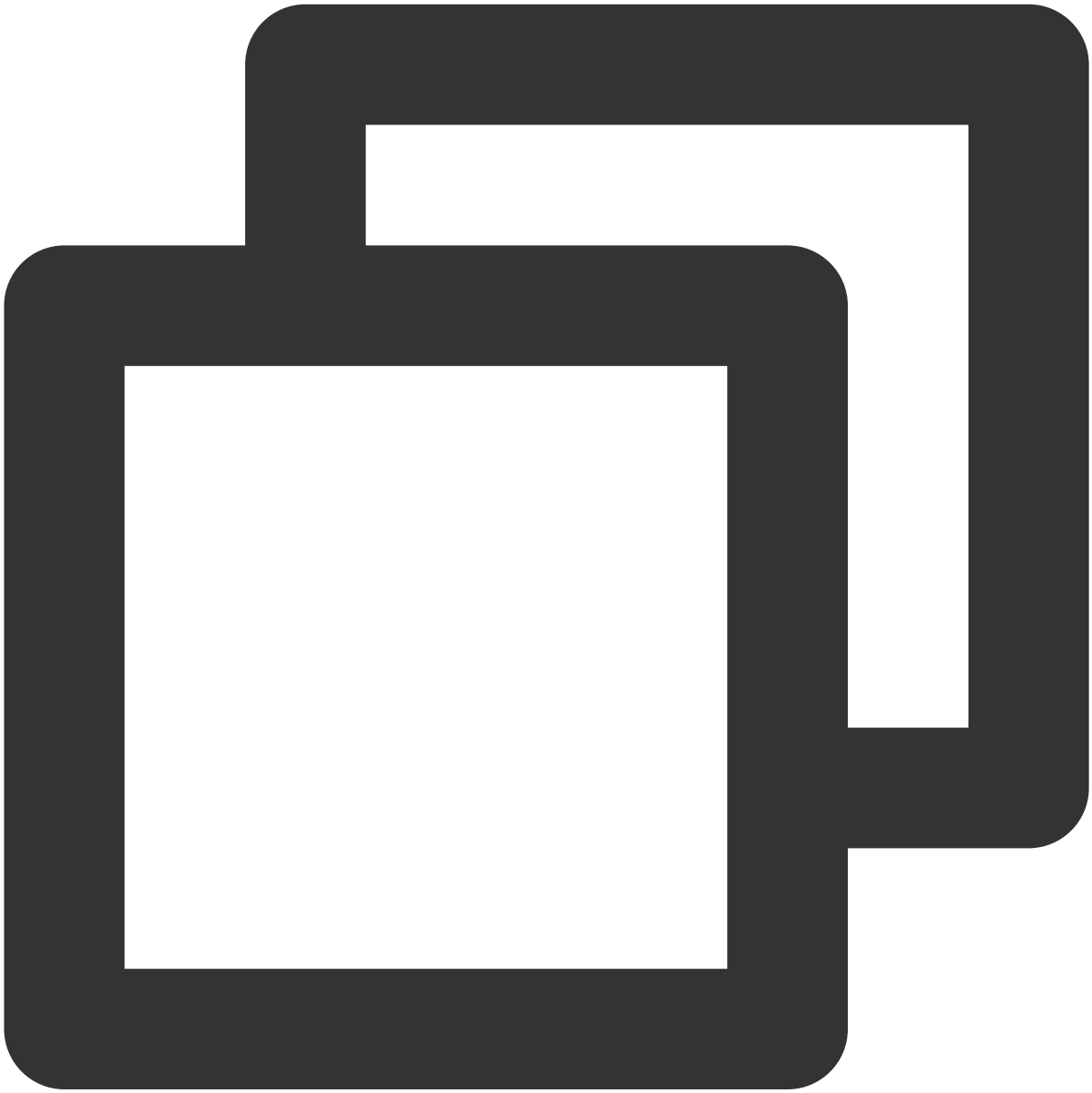
Alamat IP publik dipetakan ke alamat IP pribadi melalui NAT. Jika Anda melihat atribut antarmuka jaringan dari dalam instans (misalnya dengan menggunakan perintah seperti `ifconfig (Linux)` atau `ipconfig (Windows)`), alamat IP publik tidak ditampilkan. Untuk mendapatkan IP publik dari dalam instans, lihat Memperoleh Alamat IP Publik Instans Menggunakan Metadata Instans.

### Mendapatkan alamat IP publik dengan menggunakan API

Harap lihat DescribeInstances.

### Mendapatkan alamat IP publik menggunakan metadata instans

1. Login ke instans CVM.
Untuk informasi selengkapnya, lihat Log in ke Instans Linux dan Login ke Instans Windows.
2. Untuk mendapatkan alamat IP publik, Anda dapat mengakses metadata dengan menggunakan alat cURL atau permintaan HTTP GET.



```
curl http://metadata.tencentyun.com/meta-data/public-ipv4
```

Jika nilai yang ditampilkan dalam struktur berikut, Anda dapat melihat alamat IP publik:

```
[root@VM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/public-ipv4
115.[redacted].77.82
```

Untuk informasi selengkapnya, lihat Metadata Instans.

# Mengubah Alamat IP Publik

Waktu update terbaru：2021-12-13 17:07:04

## Ikhtisar

Dokumen ini menjelaskan cara mengubah alamat IP publik.

## Catatan

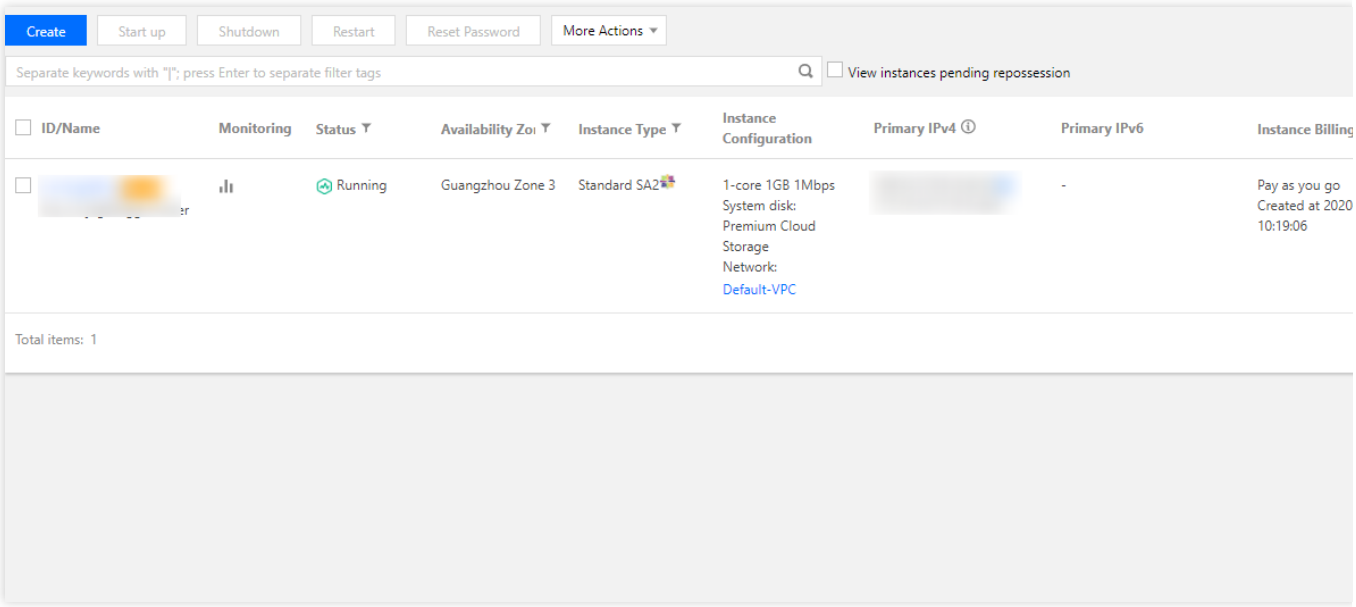
Setiap akun bisa mengubah alamat IP publik di wilayah yang sama maksimal 3 kali per hari.
Setiap instans **only change its public IP once** (hanya dapat mengubah IP publiknya sekali).
**The old public IP will be released after the change.** (IP publik lama akan dirilis setelah perubahan.)

## Prasyarat

Anda telah login ke Konsol CVM.

## Petunjuk

1. Pada halaman manajemen **Instances** (Instans), cari CVM yang ingin Anda ubah IP publiknya, klik **More** (Lainnya) -> **IP/ENI** (IP/ENI) -> **Change Public IP** (Ubah IP Publik), seperti yang ditunjukkan di bawah:




2. Di kotak dialog “Change IP” (Ubah IP), klik **Confirm** (Konfirmasi) untuk mengubah IP.

# Ambil alamat IP jaringan publik

Waktu update terbaru：2021-12-13 17:07:05

## Skenario

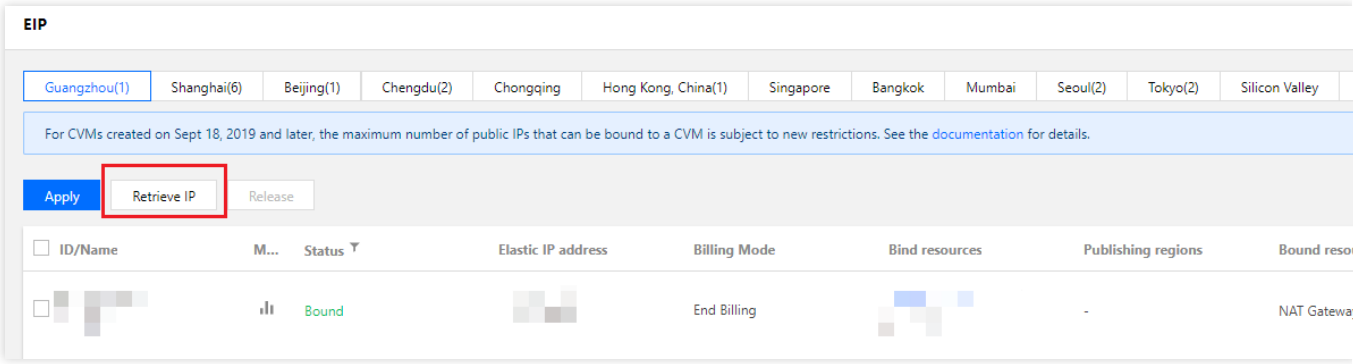
Dokumen ini menjelaskan cara mengambil alamat IP publik yang telah digunakan sebelumnya tetapi belum ditetapkan ke pengguna lain.

## Catatan

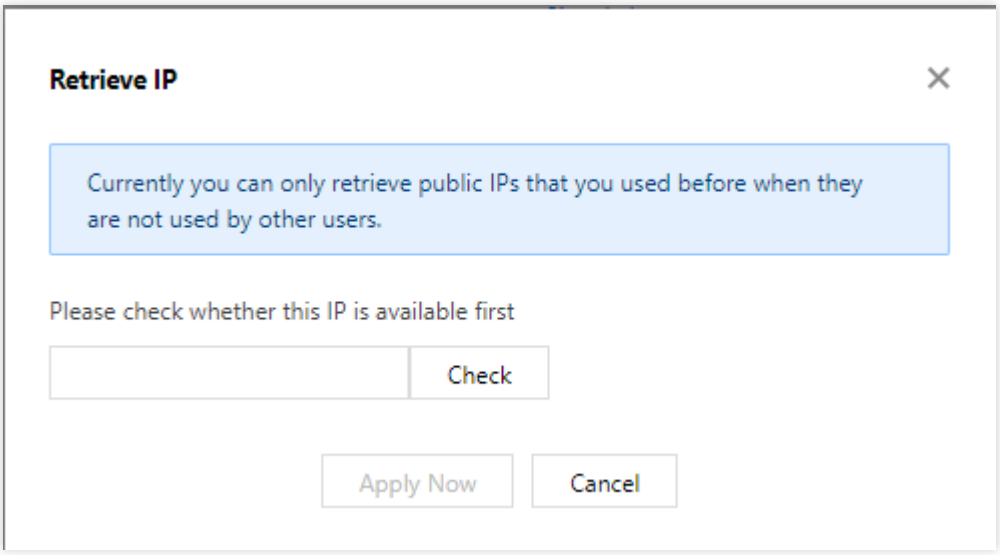
Alamat IP yang diambil adalah EIP, dan jumlah total EIP tidak boleh melebihi kuota total.
Setiap akun dapat mengajukan alamat IP tertentu hingga tiga kali per bulan di setiap wilayah.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, klik **EIP** ([EIP]) untuk mengakses halaman pengelolaan EIP.
3. Klik **Retrieve IP** (Ambil IP), seperti pada gambar berikut:




4. Di jendela pop-up **Retrieve IP** (Ambil IP), masukkan alamat IP publik dan klik **Check** (Periksa) untuk menanyakan apakah alamat IP dapat diambil, seperti yang ditunjukkan pada gambar berikut.




Jika ya, klik **Apply Now** (Terapkan Sekarang).

Jika tidak, alamat IP yang Anda ajukan tidak dapat diambil karena alasan seperti yang telah ditetapkan. Dalam hal ini, coba ajukan alamat IP lain atau klik **Cancel** (Batal) untuk keluar.

# Ubah Subnet Instans

Waktu update terbaru：2022-07-08 15:40:23

## Ikhtisar

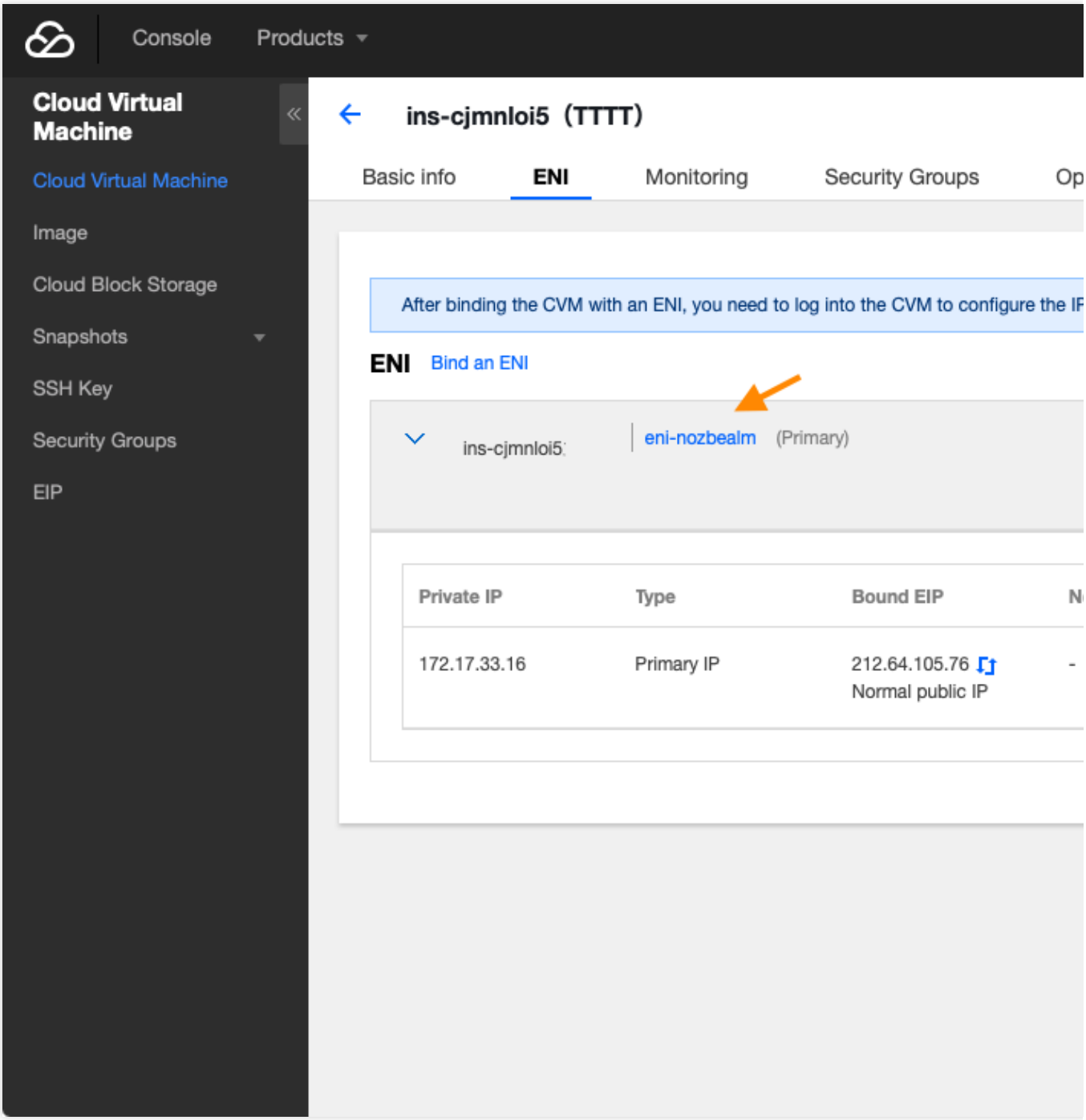
Dokumen ini menjelaskan cara mengubah subnet instans CVM di VPC melalui konsol.

## Batas

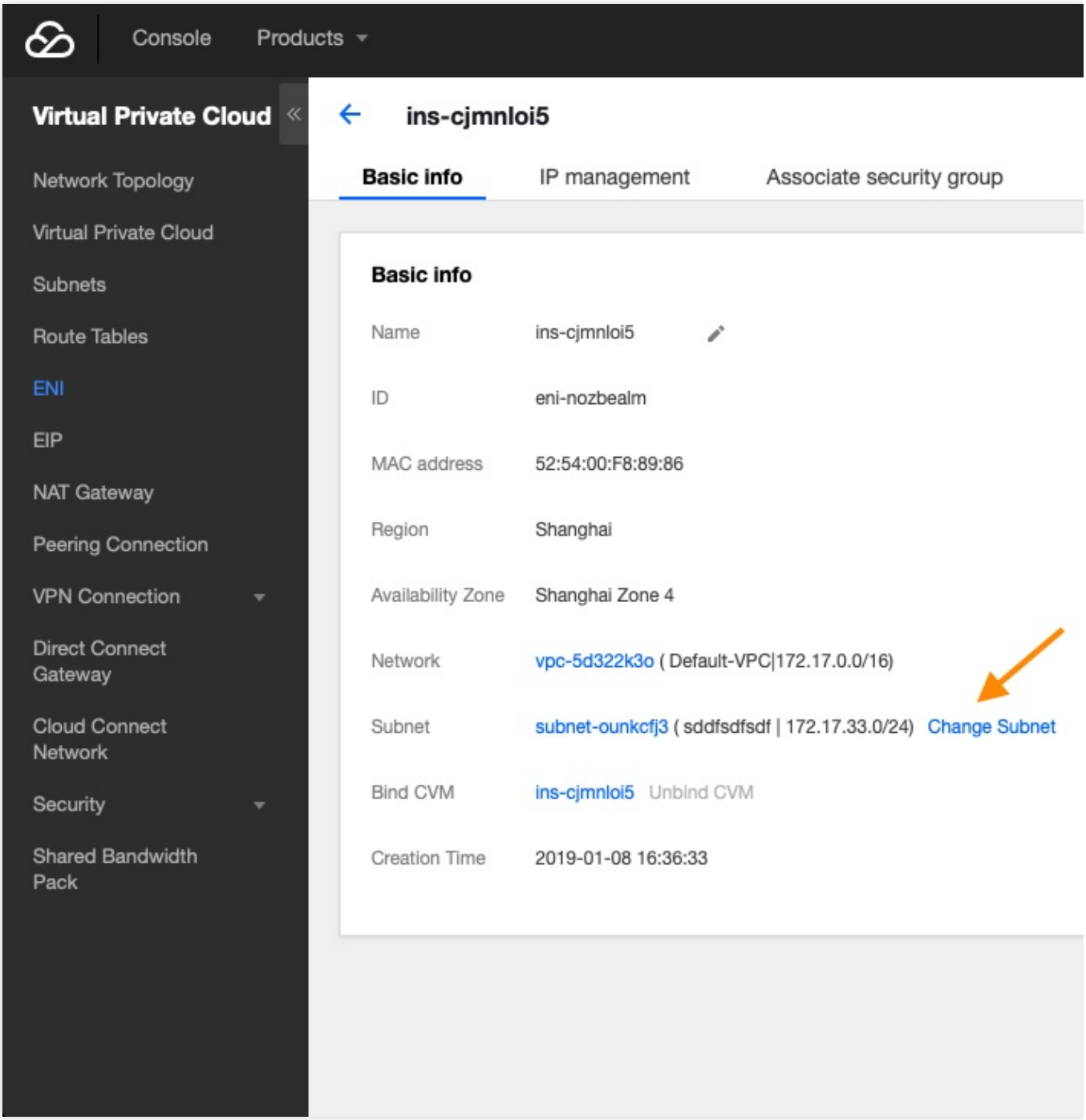
CVM terkait dimulai ulang secara otomatis setelah subnetnya diubah.
Subnet ENI sekunder tidak dapat diubah.

## Petunjuk

1. Login ke Konsol CVM.
2. Di **Instances** (Instans), pilih wilayah tempat instans yang subnetnya perlu diubah berada.
3. Temukan instans yang subnetnya perlu diubah, klik ID/Namanya dan masuk ke halaman detail instans.
4. Pilih tab **ENI** (ENI), klik ID ENI primer, dan masuk ke halaman manajemen ENI, seperti yang ditunjukkan di bawah ini:




5. Klik **Change Subnet** (Ubah Subnet), seperti yang ditunjukkan di bawah ini:

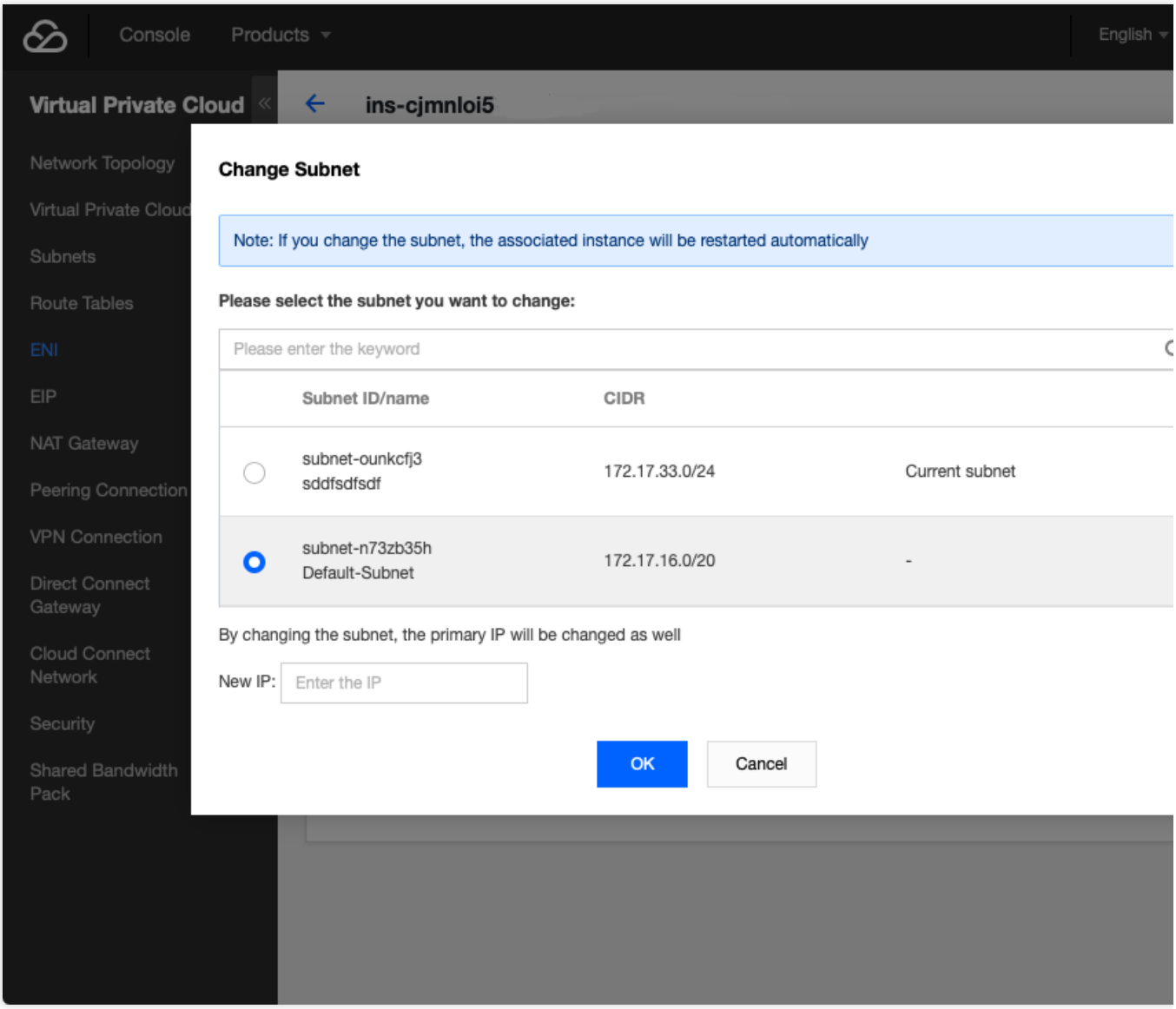



6. Pilih subnet baru di kotak pop-up. Masukkan IP baru, lalu klik **OK** (OKE), seperti yang ditunjukkan di bawah ini: Konfigurasi akan berlaku setelah instans dimulai ulang.

**Keterangan:**

Buat subnet jika tidak ada subnet yang dapat ditemukan di zona ketersediaan ini.

Hanya alamat IP pribadi dari CIDR subnet saat ini yang dapat digunakan sebagai IP baru.



# Ubah Grup Keamanan

Waktu update terbaru：2021-12-13 17:07:05

## Skenario Operasi

Grup keamanan adalah firewall virtual guna memfilter paket dan digunakan untuk mengatur kontrol akses jaringan untuk satu atau beberapa CVM. Ini adalah metode isolasi keamanan jaringan penting yang disediakan oleh Tencent Cloud. Saat membuat instans CVM, Anda harus mengonfigurasi grup keamanannya. Tencent Cloud memungkinkan Anda mengonfigurasi grup keamanan baru untuk instans CVM setelah dibuat.

**Keterangan:**

Untuk mengonfigurasi grup keamanan baru untuk instans, buat grup keamanan terlebih dahulu. Untuk informasi selengkapnya, lihat Membuat Grup Keamanan.

## Prasyarat

Login ke Konsol CVM.

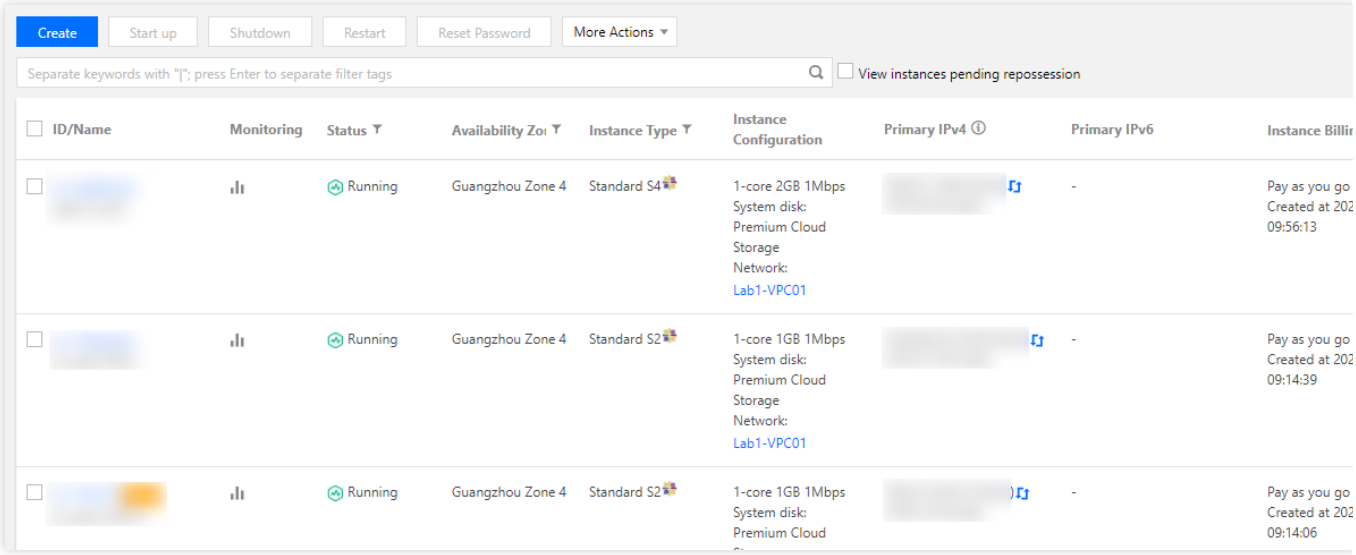
## Petunjuk

### Mengubah grup keamanan yang dikonfigurasi

Untuk meningkatkan pengalaman Anda di Konsol CVM, grup keamanan dapat dikonfigurasi di halaman manajemen instans atau di halaman detail instans.

#### Mengonfigurasi grup keamanan di halaman manajemen instans

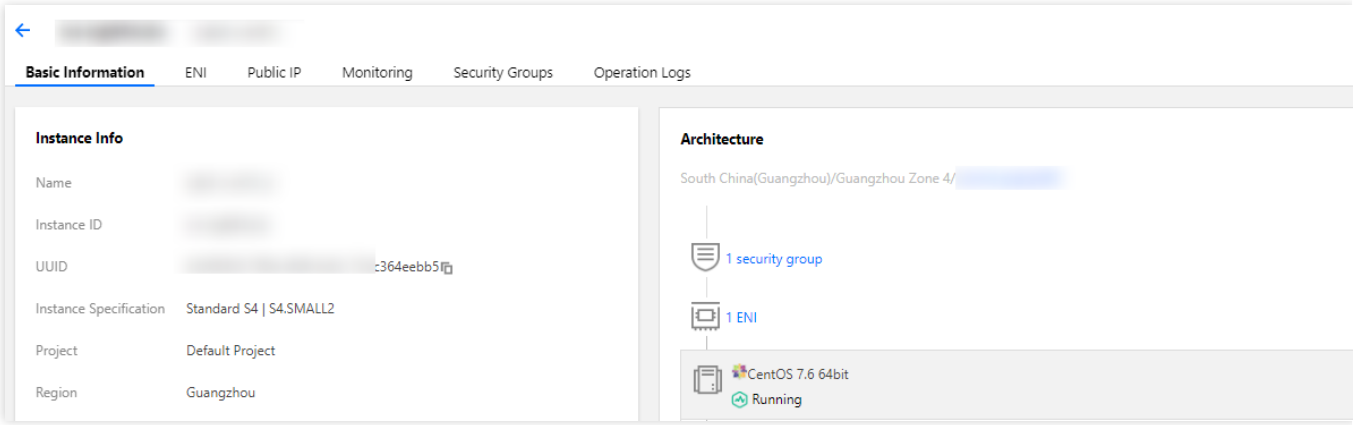
1. Pilih CVM yang akan ditetapkan ulang ke grup keamanan baru di halaman manajemen instans dan klik **More** (Lainnya) > **Security Groups** (Grup Keamanan) > **Configure Security Groups** (Konfigurasi Grup Keamanan), seperti yang ditunjukkan di bawah ini:




2. Pada jendela pop-up “Configure Security Group” (Konfigurasi Grup Keamanan), periksa nama grup keamanan baru (beberapa nama dapat dipilih) dan klik **Confirm** (Konfirmasi) untuk mengubah grup keamanan.

### Mengonfigurasi grup keamanan di halaman detail instans

1. Pada halaman manajemen instans, klik ID/nama instans CVM yang ingin Anda ubah grup keamanannya dan masuk ke halaman detail instans.
2. Klik **More Actions** (Tindakan Lainnya) > **Security Groups** (Grup Keamanan) > **Configure Security Groups** (Konfigurasi Grup Keamanan) di sudut kanan atas halaman detail instans, seperti yang ditunjukkan di bawah ini:

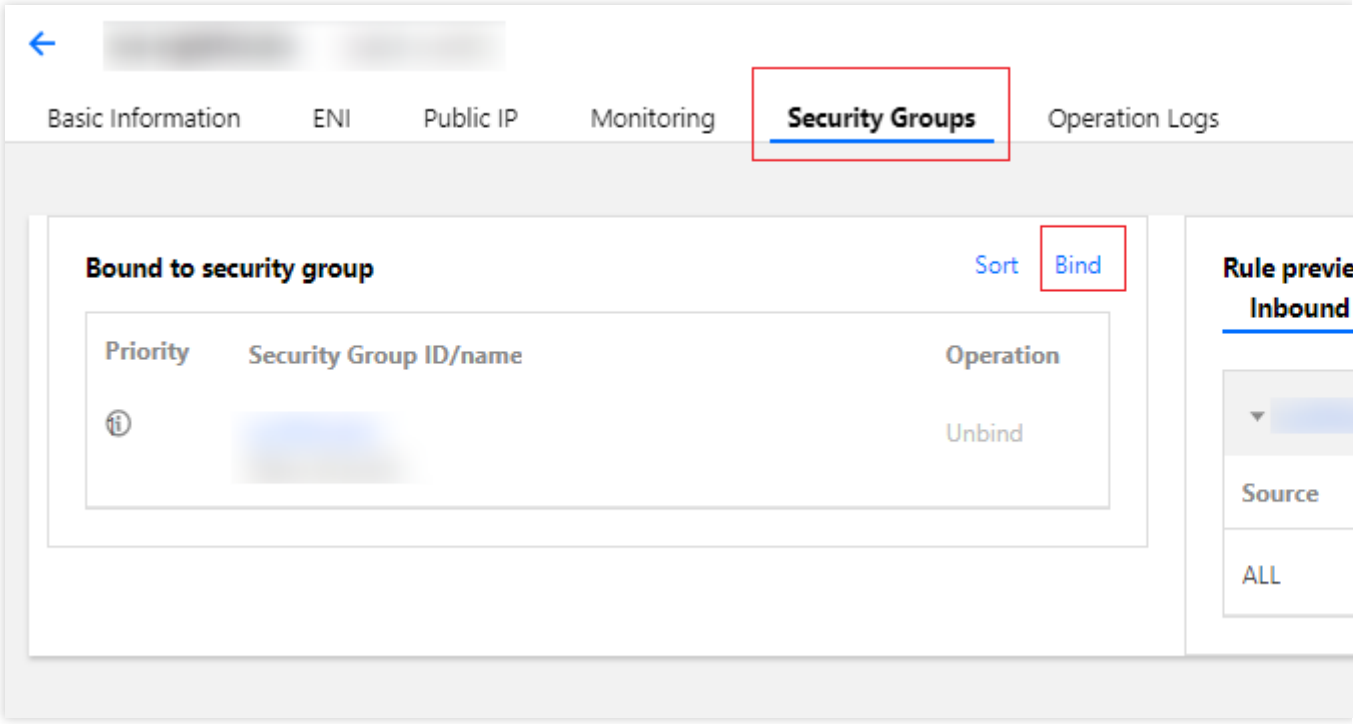



3. Pada jendela pop-up “Configure Security Group” (Konfigurasi Grup Keamanan), periksa nama grup keamanan baru (beberapa nama dapat dipilih) dan klik **Confirm** (Konfirmasi).

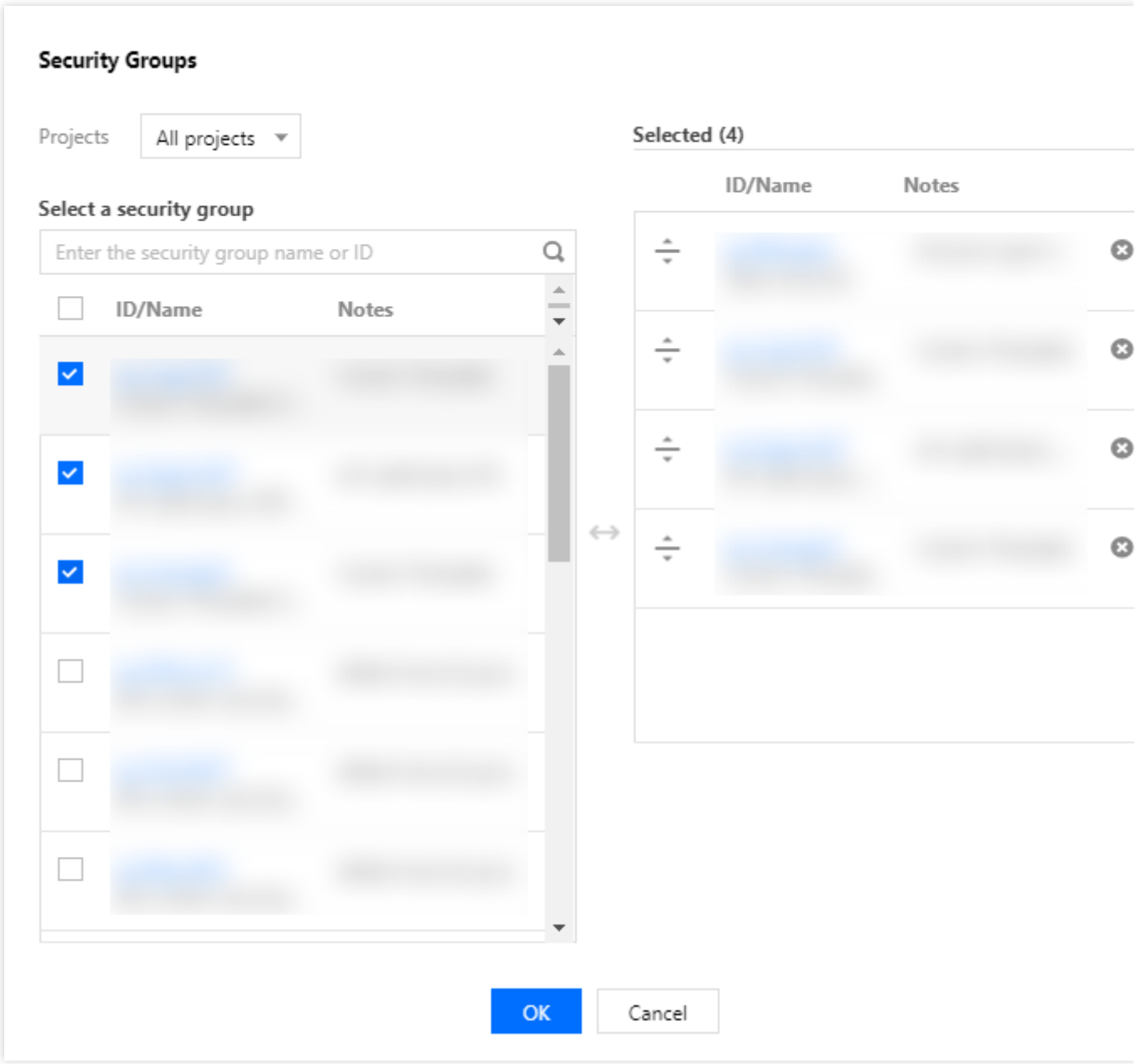
## Mengubah grup keamanan terikat

1. Pada halaman manajemen instans, klik ID/nama instans CVM yang ingin Anda ikat grup keamanannya dan masuk ke halaman detail instans.

2. Pada halaman detail instans, pilih tab **Security Groups** (Grup Keamanan) dan klik **Bind** (Ikat) pada kolom “Ikat ke grup keamanan”, seperti yang ditunjukkan di bawah ini:




3. Pada jendela pop-up “Security Groups” (Grup Keamanan), centang nama grup keamanan (beberapa nama dapat dipilih) untuk diikat berdasarkan kebutuhan Anda yang sebenarnya, lalu klik **OK** (OKE) untuk mengikat grup keamanan.



# Penggantian instans berbasis pemakaian menjadi langganan bulanan atau tahunan

Waktu update terbaru：2024-03-14 14:44:57

## Skenario pengoperasian

Untuk memudahkan Anda menggunakan CVM, Tencent Cloud telah membuka fungsi mengganti instans berbasis pemakaian CVM menjadi instans langganan bulanan atau tahunan, dan mengubah instans berbasis pemakaian untuk penggunaan sementara menjadi instans langganan bulanan atau tahunan untuk penggunaan jangka panjang dan stabil. Anda dapat menggantinya di konsol CVM dan Tencent Cloud API. Dokumen ini memperkenalkan operasi fungsional untuk mengganti instans berbasis pemakaian menjadi instans langganan bulanan atau tahunan di konsol CVM.

## Aturan Penggantian

Kami menawarkan fungsi penggantian mode penagihan di konsol CVM, dan aturan spesifiknya adalah sebagai berikut:
Mendukung penggantian tunggal dan batch untuk instans berbasis pemakaian menjadi instans langganan bulanan atau tahunan.
Pesanan perpanjangan akan dibuat saat mengonversi instans berbasis pemakaian menjadi langganan bulanan atau tahunan, dan proses pembayaran untuk pesanan ini harus diselesaikan sebelum perubahan metode penagihan diterapkan.
Jika pembayaran tidak dilakukan atau pembayaran gagal, pesanan ini dapat dilihat dan diproses di halaman Pusat Pesanan Anda.
CVM yang mode penagihannya diganti dari bayar sesuai pemakaian menjadi langganan bulanan atau tahunan tidak mendukung pengembalian tanpa alasan dalam waktu lima hari.
Setelah penggantian metode penagihan dan pembayaran berhasil, instans akan segera dikenakan biaya sesuai langganan bulanan atau tahunan. Waktu mulai instans langganan bulanan atau tahunan baru adalah waktu keberhasilan penggantian.
Sebelum pembayaran berhasil, CVM tidak dapat diganti ke mode penagihan berulang.
Sebelum pembayaran berhasil, jika ada perubahan pada informasi konfigurasi instans (seperti menyesuaikan konfigurasi/menginstal ulang sistem/menyesuaikan bandwidth/menyesuaikan disk, dll.), jumlah pesanan pembelian baru tidak sesuai dengan instans, maka pembayaran untuk pesanan yang belum dibayar akan dihentikan, Anda harus membatalkan pesanan yang belum dibayar saat ini di Pusat Pesanan sebelum melakukan penggantian baru.

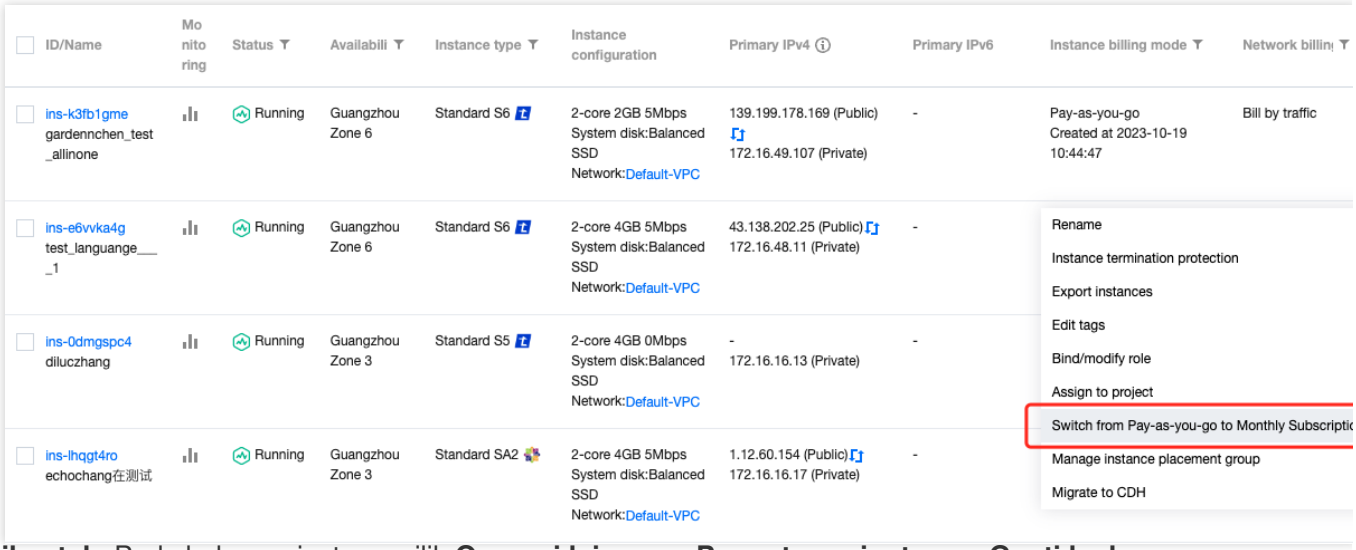
Fungsi penggantian bayar sesuai pemakaian menjadi langganan bulanan atau tahunan mendukung penggantian sinkron mode penagihan instans dan disk. Setelah mode penagihan instans diganti, mode penagihan bandwidth jaringan tetap tidak berubah kecuali untuk mode penagihan bandwidth per jam dari IP publik biasa untuk jenis akun standar (bill-by-IP) dan mode penagihan bandwidth per jam dari jenis akun tradisional (bill-by-CVM) yang mendukung penggantian otomatis menjadi penagihan bulanan atau tahunan berdasarkan bandwidth.

## Batasan pemakaian

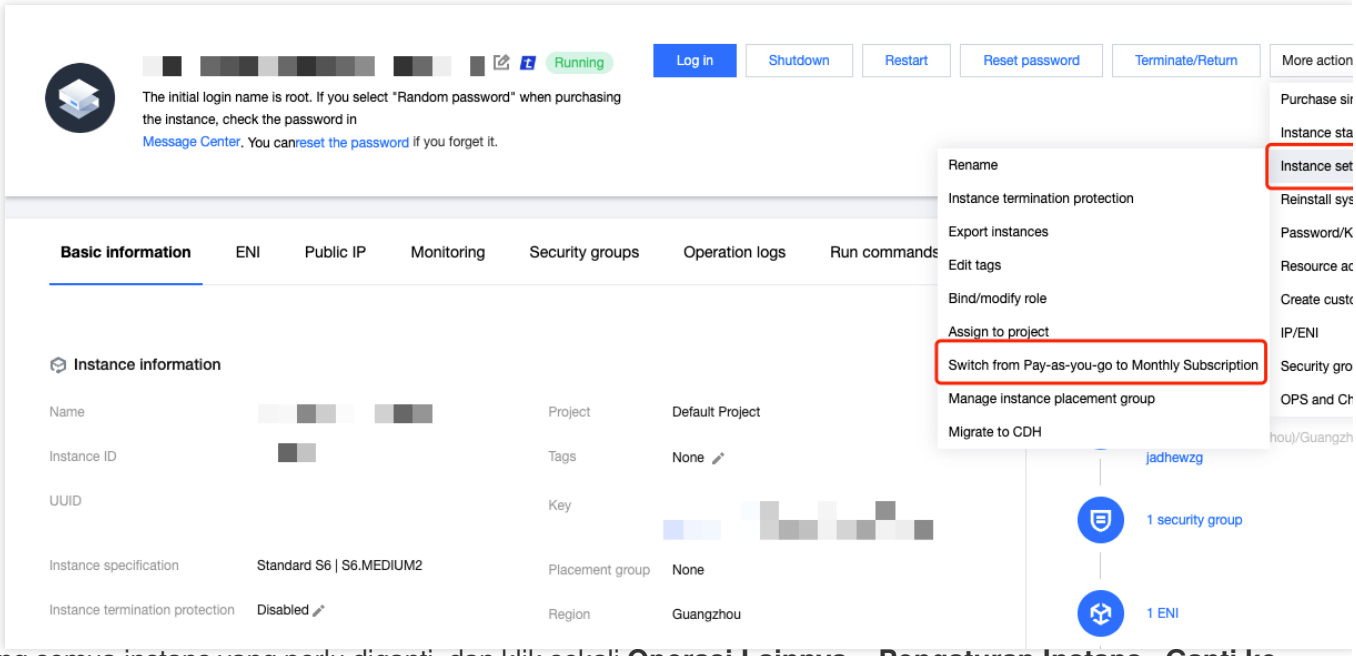
Penggantian tidak didukung jika sisa kuota langganan bulanan atau tahunan di zona ketersediaan kurang dari jumlah instans berbasis pemakaian yang akan diganti.
Instans bukan bayar sesuai pemakaian tidak mendukung penggantian.
Instans spot tidak mendukung penggantian.
Mode penagihan jaringan instans didasarkan pada durasi penggunaan bandwidth, dan saat ini tidak mendukung penggantian.
Instans yang menggunakan gambar pasar cloud tidak mendukung penggantian.
Instans batch BC1, BS1 tidak mendukung penggantian.
Instans berbasis pemakaian memiliki pesanan penggantian yang belum dibayar dan tidak mendukung penggantian.
Instans berbasis pemakaian telah diatur untuk pemusnahan terjadwal dan tidak mendukung penggantian. Jika penggantian diperlukan, harap batalkan pemusnahan terjadwal dulu sebelum melakukan penggantian lagi.

## Langkah-langkah pengoperasian

1. Login Konsol Cloud Virtual Machine.
2. Sesuai dengan kebutuhan aktual, pilih operasi instans penggantian yang berbeda di halaman manajemen instans.
Mengganti satu instans
Mengganti beberapa instans
Di halaman manajemen instans, operasikan sesuai dengan mode tampilan aktual yang digunakan:
**Tampilan Daftar**: Pada bilah operasi di sebelah kanan, pilih **Lainnya** > **Pengaturan instans** > **Ganti ke langganan bulanan atau tahunan berbasis pemakaian**. Seperti yang ditunjukkan pada gambar di bawah ini:
**Keterangan:**
Anda juga bisa mencentang instans yang perlu diganti, dan klik sekali **Operasi lainnya**> **Pengaturan instans** > **Ganti ke langganan bulanan atau tahunan berbasis pemakaian** di bagian atas.

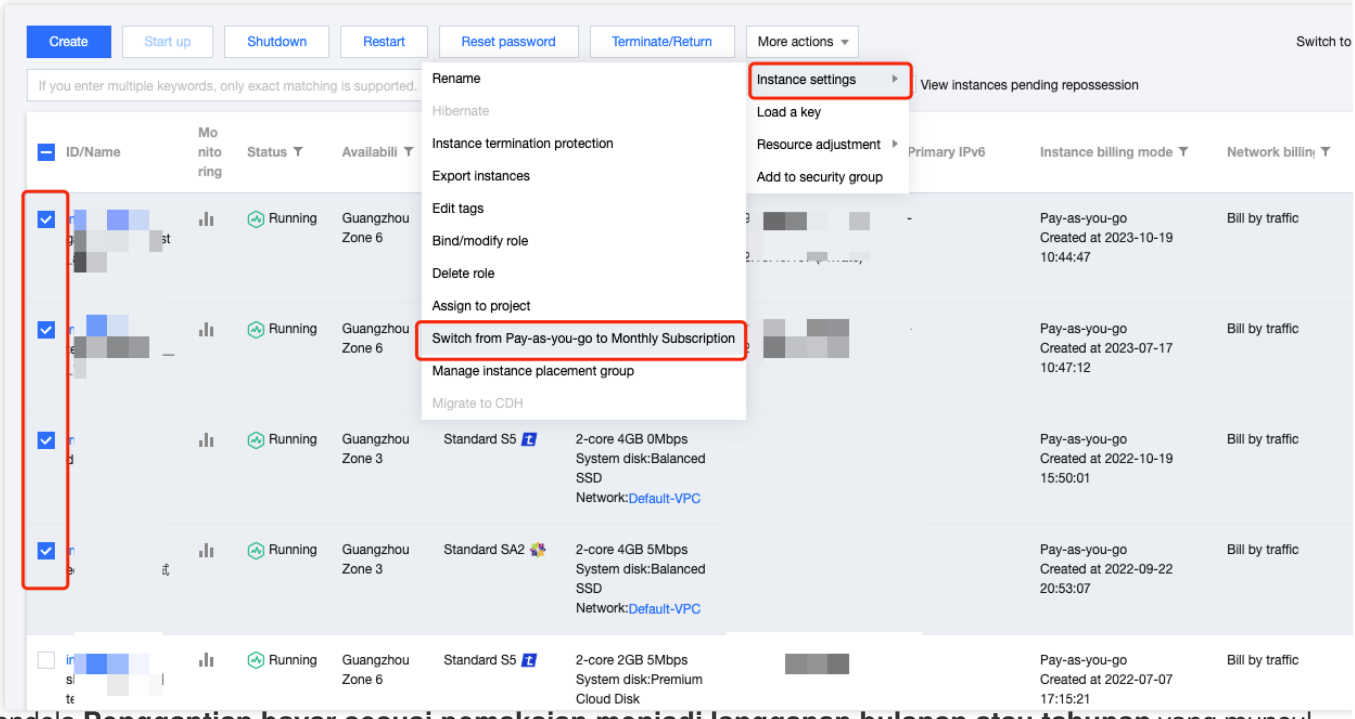



**Tampilan tab**: Pada halaman instans, pilih **Operasi lainnya** > **Pengaturan instans** > **Ganti ke langganan bulanan atau tahunan berbasis pemakaian**. Seperti yang ditunjukkan pada gambar di bawah ini:

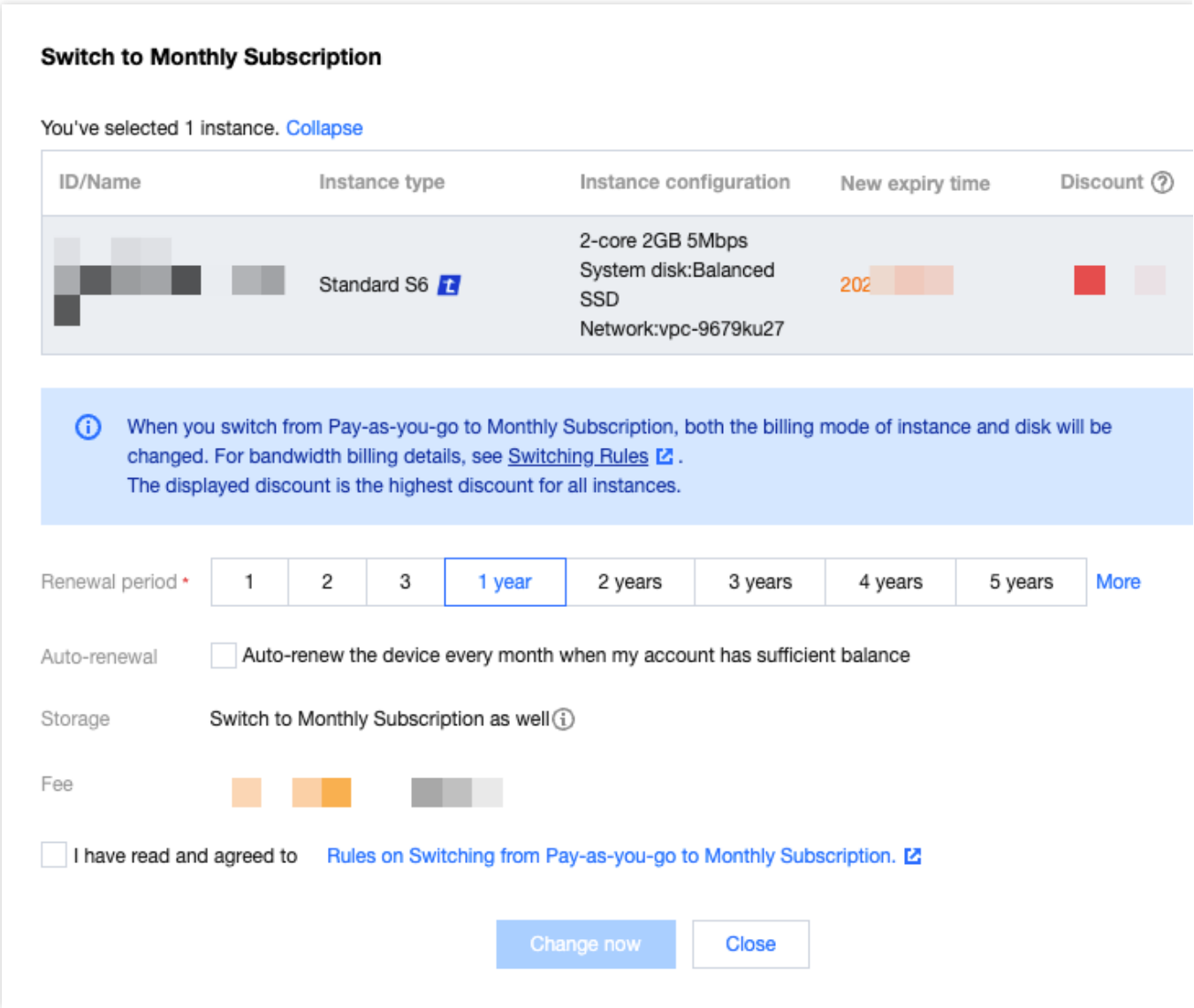



Centang semua instans yang perlu diganti, dan klik sekali **Operasi Lainnya** > **Pengaturan Instans**> **Ganti ke langganan bulanan atau tahunan berbasis pemakaian** di bagian atas. Anda dapat mengganti mode penagihan instans secara batch. Seperti yang ditunjukkan pada gambar di bawah ini:

Alasan akan ditampilkan jika instans tidak dapat dioperasikan.




3. Di jendela **Penggantian bayar sesuai pemakaian menjadi langganan bulanan atau tahunan** yang muncul, atur durasi perpanjangan dan apakah akan otomatis diperpanjang berdasarkan kebutuhan aktual. Seperti yang ditunjukkan pada gambar di bawah ini:




Durasi perpanjangan: Pilih durasi pembelian setelah diganti menjadi langganan bulanan atau tahunan. Jika beberapa instans diganti dalam batch, hanya durasi pembelian yang sama yang dapat diatur.

Perpanjangan otomatis: Pilih perpanjangan otomatis sesuai kebutuhan Anda.

4. Centang **Saya telah membaca dan menyetujui aturan penggantian bayar sesuai pemakaian menjadi langganan bulanan atau tahunan**, dan klik sekali **Ganti sekarang**.

Jika tidak ada pesanan penggantian yang belum dibayar untuk instans ini, maka akan otomatis lompat ke halaman pembayaran.

5. Menyelesaikan pembayaran sesuai petunjuk di halaman berarti menyelesaikan penggantian.

# Masalah Umum

Jika Anda mengalami masalah selama proses penggantian, silakan lihat Masalah Umum > Mengenai Penagihan dalam dokumen.

# Cari Instans

Waktu update terbaru：2021-12-13 17:07:05

## Skenario

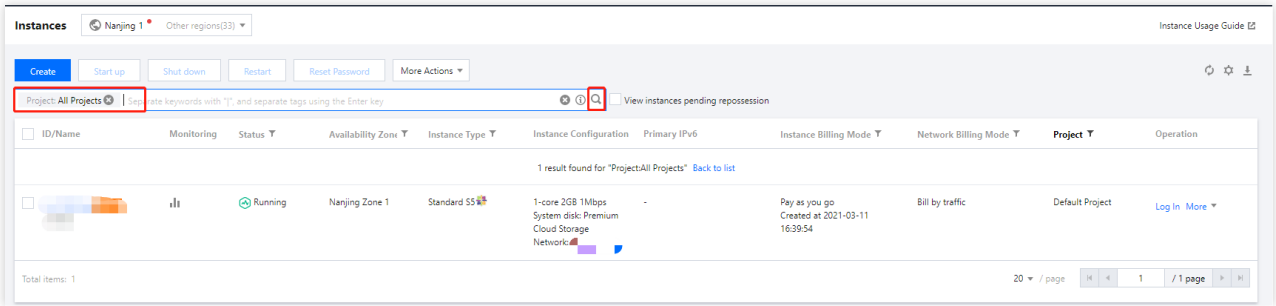
Secara default, konsol CVM menampilkan instans untuk semua proyek di wilayah saat ini. Untuk membantu Anda mencari instans di wilayah saat ini dengan cepat, Tencent Cloud menyediakan fitur pencarian CVM. Anda dapat memfilter instans berdasarkan atribut sumber daya seperti proyek, metode penagihan instans, jenis instans, zona ketersediaan, IP, ID instans, dan nama instans.

## Petunjuk

1. Login ke Konsol CVM.
2. Masukkan konten yang ingin Anda cari berdasarkan kebutuhan Anda, dan klik

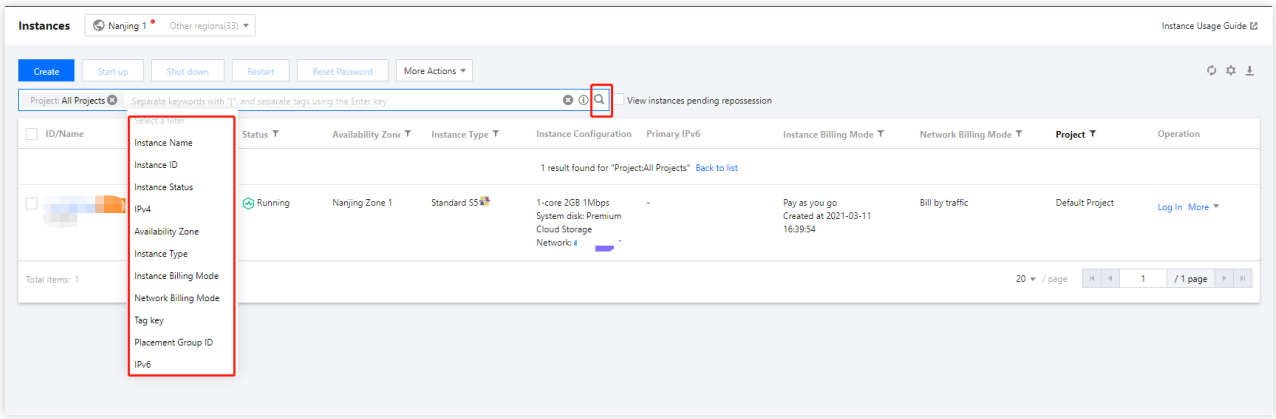
untuk mencari.
Masukkan kata kunci di kotak teks pencarian, dan klik

, seperti yang ditunjukkan di bawah ini:




Pilih dimensi tertentu untuk dicari (seperti proyek, proyek, metode penagihan instans, jenis instans, dll.) dan klik

, seperti yang ditunjukkan di bawah ini:




3. Untuk mempelajari selengkapnya tentang sintaksis pencarian, klik

untuk melihat sintaksis yang relevan dari instans pencarian.

Untuk sintaksis instans pencarian lebih lanjut, harap lihat gambar berikut.

| | Enter Format | Example | Display in Search Box | Description |
|---|---|---|---|---|
| Single keyword | [Keyword] | 10.0.0.1 | 10.0.0.1 Use '\|' to split more than one keywor | List all instances including the keyword “10.0.0.1” |
| Multiple keywords | [Keyword] [Enter key ↵] [Keyword] | 10.0.0.1<br>www.123.com<br>192.169.23.54 | 10.0.0.1 www.123.com 192.169.23.45 | List all instances that include all the three keywords“10.0.0.1”,“www.123.com”and“192.169.23.54” |
| Single resource type | [Resource type]:[Keyword] | IP: 10.0.0.1 | IP: 10.0.0.1 Use '\|' to split more than one key | List all instances whose IP is “10.0.0.1” |
| Multiple resource types | [Resource type]:[Keyword][ Enter key ↵][Resource type]: [Keyword] | Availability Zone: Hong Kong Zone 2<br>Project: Default | Availability Zone: Hongkon... Project: Defau | List all instances whose“Availability Zone”is“Hong Kong Zone 2” and “Project “ is “Default” |
| Single resource type and multiple keywords | [Resource type]:[Keyword] \| [Keyword] | CVM Status: Creating \| Shutdown | CVM Status: Creating \| Shu... Use '\|' to split | List all instances whose “CVM Status “ is “Creating” or “Shutdown” |
| Pasted contents | {pasted contents} | 112.11.22.33<br>112.11.22.34<br>112.11.22.53 | 112.11.22.33 \| 112.11.22.3... Use '\|' to split | List all instances include the keywords “112.11.22.33”, “112.11.22.34” or “112.11.22.53” |

# Ekspor Instans

Waktu update terbaru：2021-12-13 17:07:05

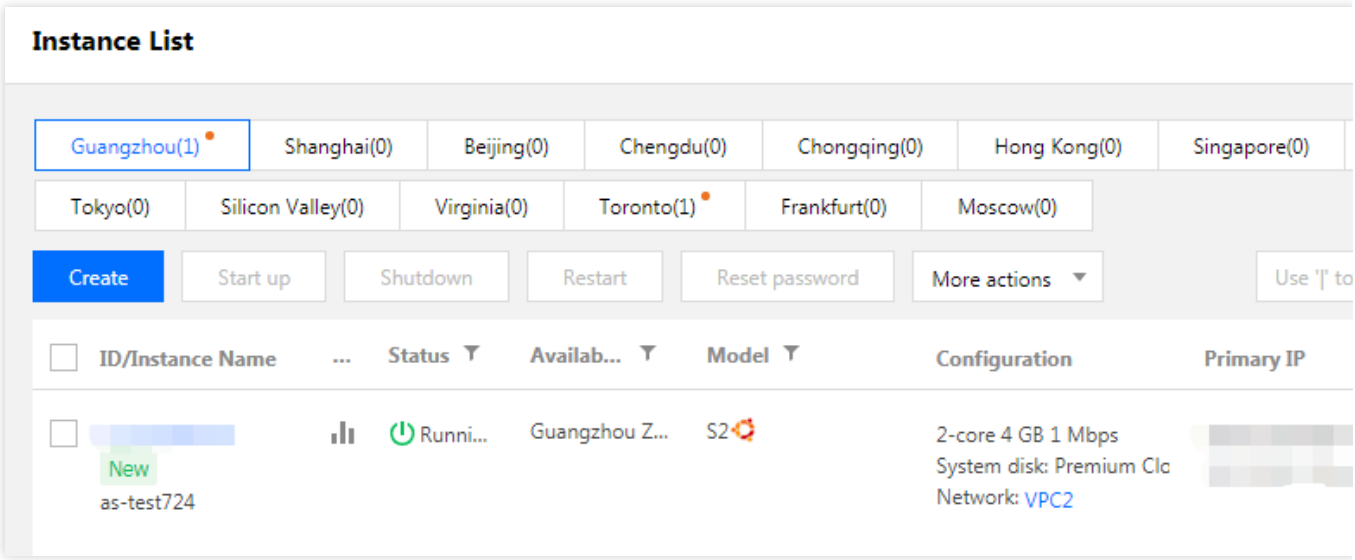
## Skenario

Anda dapat mengekspor daftar instans CVM suatu wilayah di konsol, dan menyesuaikan bidang yang akan diekspor. Anda dapat memilih maksimum 27 bidang, termasuk ID, nama instans, status, wilayah, zona ketersediaan, jenis instans, sistem operasi, ID citra, CPU, MEM, bandwidth, IP publik, IP pribadi, jenis disk sistem, ukuran disk sistem, jenis disk data, ukuran disk data, jenis jaringan, ID subnet, nama VPC, waktu pembuatan, waktu kedaluwarsa, mode penagihan instans, mode penagihan jaringan, proyek, ID host khusus, dan tag.

## Petunjuk

1. Login ke Konsol CVM.
2. Pilih wilayah.
3. Klik

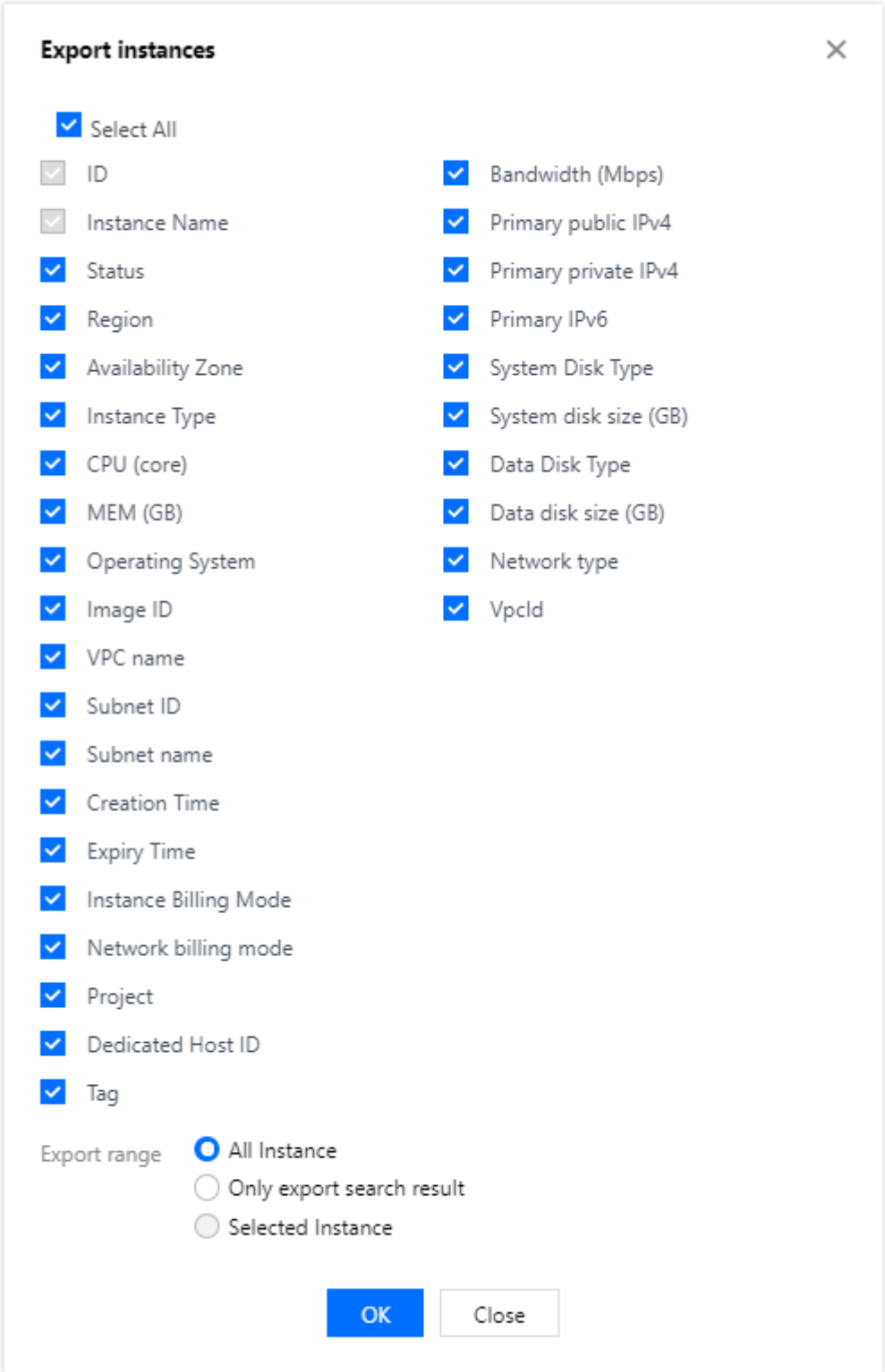
di kanan atas daftar instans, seperti yang ditunjukkan di bawah ini:




4. Di jendela pop-up “Export instances” (Ekspor instans), pilih bidang yang ingin Anda ekspor dan klik “OK”, seperti yang ditunjukkan di bawah ini:

**Keterangan:**

Anda dapat memilih maksimum 27 bidang yang akan diekspor.



# Memperbarui Instans

Waktu update terbaru：2021-12-13 17:07:05

Dokumen ini memperkenalkan cara memperpanjang **Postpaid instance** (Instans pascabayar).

- **Postpaid instance** (Instans pascabayar): Instans pascabayar dapat diaktifkan secara otomatis dengan saldo yang cukup di akun Anda. Untuk informasi selengkapnya, harap lihat Top-up Online.

# Memulai Instans

Waktu update terbaru：2021-12-13 17:07:08

## Ikhtisar

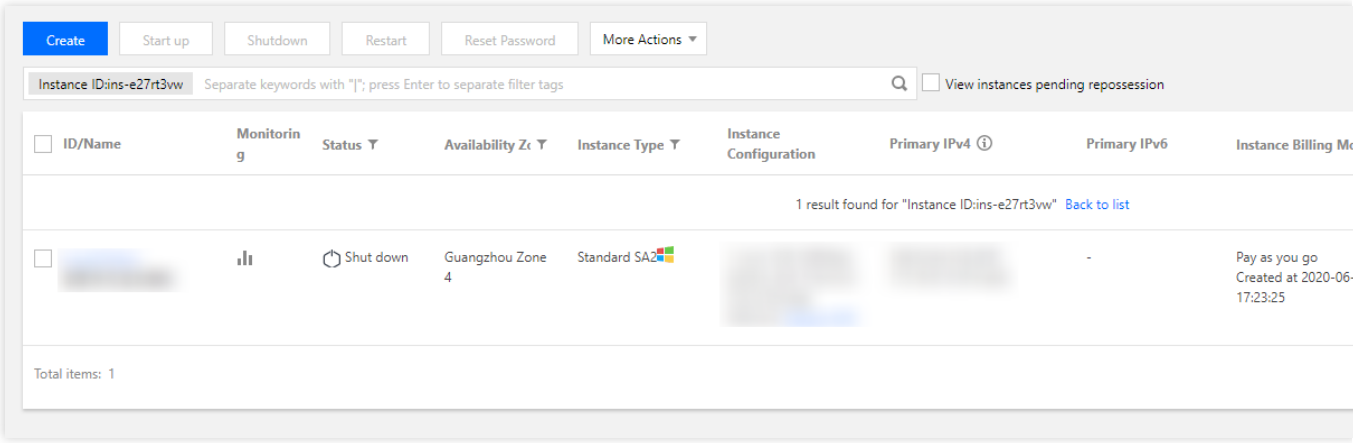
Dokumen ini menjelaskan cara memulai instans melalui konsol atau API.

## Petunjuk

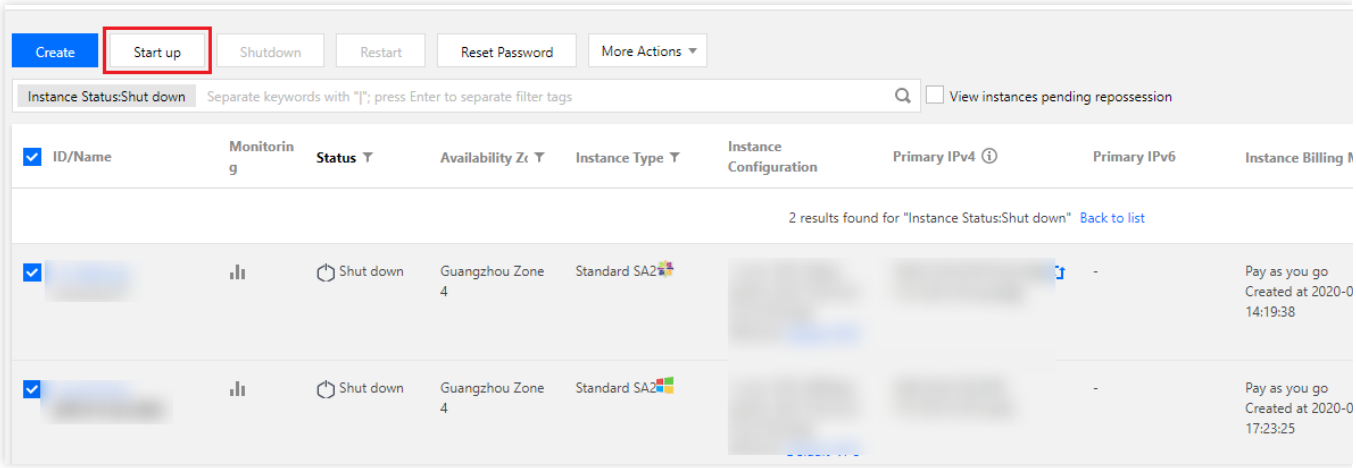
### Memulai instans melalui konsol

1. Login ke konsol CVM.
2. Pilih metode operasi yang sesuai berdasarkan kebutuhan Anda yang sebenarnya.

**Starting up one instance** (Memulai satu instans): pilih instans yang ingin Anda mulai, lalu klik **More** (Lainnya) -> **Instance Status** (Status Instans) -> **Start up** (Mulai) di kolom **Operation** (Operasi) di sebelah kanan, seperti yang ditunjukkan di bawah ini:




**Starting up the instances** (Memulai instans): pilih instans yang ingin Anda mulai, dan klik **Start up** (Mulai) di bagian atas daftar untuk memulai instans yang dipilih, seperti yang ditunjukkan di bawah ini:




### Memulai instans melalui API

Gunakan StartInstances API untuk memulai instans.

## Operasi Selanjutnya

Setelah instans dimulai, Anda dapat melakukan operasi berikut:

**Logging in to the instance** (Login ke instans): bergantung pada jenis instans, login ke instans Linux atau instans Windows.

**Initializing cloud disks** ([Menginisialisasi disk cloud]): menginisialisasi disk cloud yang dipasang ke instans dengan memformat, mempartisi, dan membuat sistem file.

# Mematikan Instans

Waktu update terbaru：2021-12-13 17:07:06

## Skenario

Instans dapat dimatikan saat Anda perlu menghentikan layanan, atau mengubah konfigurasi yang hanya dapat dilakukan dalam keadaan nonaktif. Menonaktifkan instans sama halnya seperti mematikan komputer lokal.

## Catatan

Anda dapat mematikan instans menggunakan perintah sistem (seperti perintah pematian pada sistem Windows dan sistem Linux) atau melalui konsol Tencent Cloud. Sebaiknya lihat proses pematian di konsol untuk memeriksa apakah ada masalah yang terjadi.
Instans tidak akan lagi menyediakan layanan setelah pematian. Sebelum pematian, pastikan CVM telah berhenti menerima permintaan layanan.
Selama pematian, status instans akan berubah dari "shutting down" (sedang mematikan) menjadi "shutdown" (dimatikan). Jika proses pematian memakan waktu terlalu lama, mungkin ada pengecualian. Untuk informasi selengkapnya, lihat Menutup CVM untuk menghindari pematian paksa.
Setelah instans dimatikan, semua penyimpanan masih terhubung ke instans, dan semua data disk disimpan. Data dalam memori akan hilang.
Mematikan instans tidak mengubah atribut fisiknya. IP publik dan pribadi dari instans tetap tidak berubah. IP Publik Elastis masih terikat ke instans. Namun, karena gangguan layanan, Anda akan menerima respons kesalahan saat mengakses IP ini. Hubungan Classiclink tetap tidak berubah.
Jika instans milik kluster server nyata dari instans CLB, instans tersebut tidak dapat lagi menyediakan layanan setelah pematian.
Jika kebijakan pemeriksaan kesehatan telah dikonfigurasi, instans yang telah dimatikan akan diblokir secara otomatis dan permintaan tidak akan lagi diteruskan. Jika tidak, klien mungkin menerima kode kesalahan 502. Untuk informasi selengkapnya, lihat Pemeriksaan Kesehatan.
Jika instans yang telah dimatikan berada dalam grup penskalaan otomatis, layanan penskalaan otomatis akan menandai instans memiliki kinerja yang buruk, dan dapat mengganti dan memindahkannya dari grup penskalaan otomatis. Untuk informasi selengkapnya, lihat Penskalaan Otomatis.

## Petunjuk

### Mematikan instans melalui konsol

1. Login ke Konsol CVM.
2. Pilih metode yang berbeda berdasarkan kebutuhan aktual.

Mematikan instans: pilih instans yang akan dimatikan, lalu klik **More**(Lainnya)>**Instance Status**(Status Instans)> **Shutdown**(Matikan)di kolom operasi di sisi kanan.

Mematikan beberapa instans: pilih semua instans untuk dimatikan, lalu klik **Shutdown** (Matikan) di bagian atas daftar untuk mematikan instans dalam batch.

Alasan diberikan untuk instans yang tidak dapat dionaktifkan.

### Mematikan instans melalui API

Untuk informasi selengkapnya, lihat StopInstances API.

## Operasi Selanjutnya

Anda dapat mengubah atribut berikut hanya jika instans telah dimatikan.

**Instance configuration (CPU, memory):** (Konfigurasi instans (CPU, memori):) Untuk mengubah jenis instans, lihat Ubah Konfigurasi Instans.

**Change password** (Ubah kata sandi:) lihat Kata Sandi Login.

**Load SSH key:** (Muat kunci SSH:) lihat Kunci SSH.

# Memulai Ulang Instans

Waktu update terbaru：2021-12-13 17:07:06

## Skenario Operasi

Memulai ulang instans CVM adalah metode umum untuk memeliharanya. Langkah ini sama dengan memulai ulang sistem operasi komputer lokal. Dokumen ini menjelaskan cara memulai ulang instans.

## Catatan

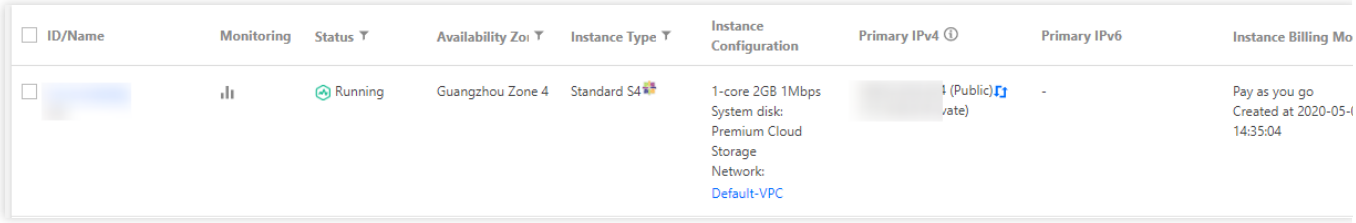
**Preparing to restart instances:** (Mempersiapkan untuk memulai ulang instans:) Instans tidak dapat menyediakan layanan selama proses mulai ulang. Pastikan sebelum memulai ulang CVM bahwa instans telah berhenti menerima permintaan layanan.
**How to restart instances:** (Cara memulai ulang instans:) Sebaiknya mulai ulang instans menggunakan operasi mulai ulang yang disediakan oleh Tencent Cloud, bukan menjalankan perintah mulai ulang di instans (seperti perintah luncurkan ulang di Windows dan perintah boot ulang di Linux).
**Restart time:** (Waktu mulai ulang:) Umumnya, dibutuhkan hanya beberapa menit untuk memulai ulang instans.
**Physical features of instances:** (Fitur fisik instans:) Memulai ulang instans tidak mengubah fitur fisiknya. Alamat IP publik dan pribadinya serta data yang disimpan tidak akan diubah.
**Billing:** (Penagihan:) Memulai ulang instans tidak akan memulai periode penagihan instans baru.

## Petunjuk

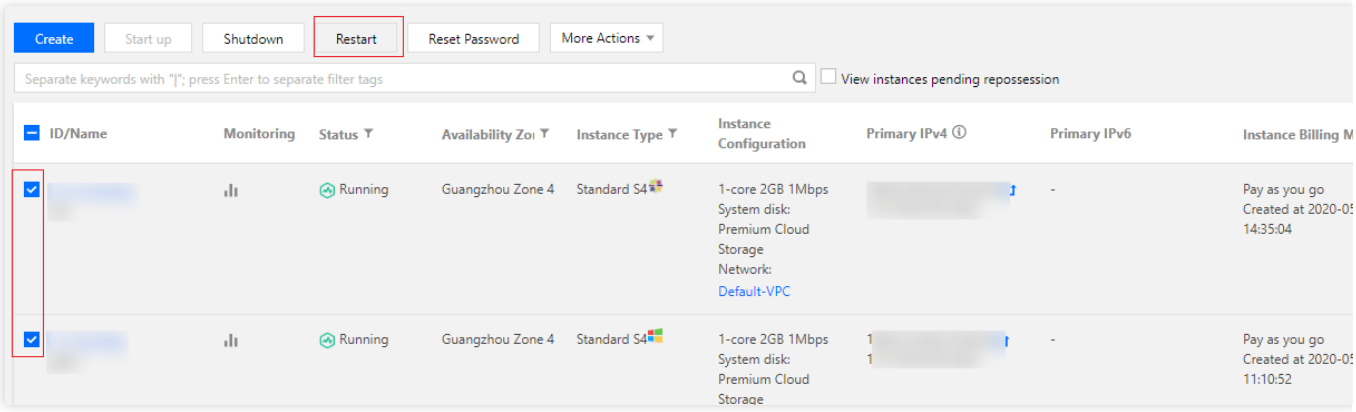
Anda dapat memulai ulang instans melalui metode berikut:
Gunakan konsol untuk memulai ulang instans
Gunakan API untuk memulai ulang instans

### Menggunakan konsol untuk memulai ulang instans

1. Login ke Konsol CVM.
2. Pada halaman manajemen instans, pilih metode mulai ulang instans berdasarkan jumlah aktual instans yang akan dimulai ulang.
Memulai ulang satu instans: Pada baris instans yang ingin Anda mulai ulang, klik **More** (Lainnya) > **Instance Status** (Status Instans) > **Restart** (Mulai Ulang), seperti yang ditunjukkan di bawah ini:




Memulai ulang beberapa instans: Centang semua instans yang ingin Anda mulai ulang, lalu klik **Restart** (Mulai Ulang) di bagian atas daftar untuk memulai ulang instans secara massal. Jika tidak dapat dimulai ulang, alasannya akan ditampilkan, seperti yang ditunjukkan di bawah ini:




**Keterangan:**

Satu instans juga dapat dimulai ulang menggunakan metode ini.

## Menggunakan API untuk memulai ulang instans

Lihat RebootInstances API.

# Menginstal Ulang Sistem

Waktu update terbaru：2021-12-13 17:07:07

## Ikhtisar

Penginstalan ulang sistem adalah metode penting untuk mengembalikan instans ke status awal jika terjadi kegagalan sistem.

CVM mendukung dua jenis penginstalan ulang berikut:

**Single-system reinstallation** (Penginstalan ulang sistem tunggal): CVM di semua wilayah dapat diinstal ulang ke sistem operasi yang sama.

Misalnya, Linux diinstal ulang sebagai Linux dan Windows diinstal ulang sebagai Windows.

**Cross-system reinstallation** (Penginstalan ulang lintas sistem): hanya CVM di daratan China (tidak termasuk Hong Kong, China) yang dapat diinstal ulang ke sistem operasi yang berbeda.

Misalnya, Linux diinstal ulang sebagai Windows dan Windows diinstal ulang sebagai Linux.

**Keterangan:**

Saat ini, semua instans CBS baru dan disk lokal mendukung penginstalan ulang lintas sistem. Namun, beberapa disk lokal 20 GB yang ada tidak mendukung penginstalan ulang lintas sistem melalui Konsol. Jika Anda perlu menerapkan penginstalan ulang lintas sistem untuk instans pada disk lokal ini, harap kirim tiket untuk mengajukan fitur penginstalan lintas sistem.

Instans spot tidak mendukung penginstalan ulang sistem.

## Catatan

**Preparing for reinstallation:** (Mempersiapkan penginstalan ulang:) cadangkan data penting ke disk sistem Anda sebelum penginstalan ulang karena data disk sistem akan hilang setelah penginstalan ulang. Untuk menyimpan data sistem Anda, sebaiknya buat citra kustom dan gunakan citra ini untuk menginstal ulang sistem.

**Image selection:** (Pemilihan citra:) sebaiknya gunakan citra yang disediakan oleh Tencent Cloud atau citra kustom Anda, bukan citra dari sumber yang tidak dikenal atau sumber lain. Jangan lakukan operasi lain saat disk sistem sedang diinstal ulang.

**Instance physical features:** (Fitur fisik instans:) IP publik instans tidak akan berubah.

**Billing:** (Penagihan:) saat menyesuaikan ukuran disk sistem (hanya untuk CBS), Anda akan dikenakan biaya sesuai dengan standar harga CBS. Untuk informasi selengkapnya, lihat Daftar Harga.

**Subsequent operations:** (Operasi selanjutnya:) setelah disk sistem diinstal ulang, data dalam disk data tidak akan terpengaruh dan hanya akan tersedia untuk digunakan setelah disk data dipasang kembali.

# Petunjuk

Anda dapat menggunakan salah satu metode berikut untuk menginstal ulang sistem operasi:

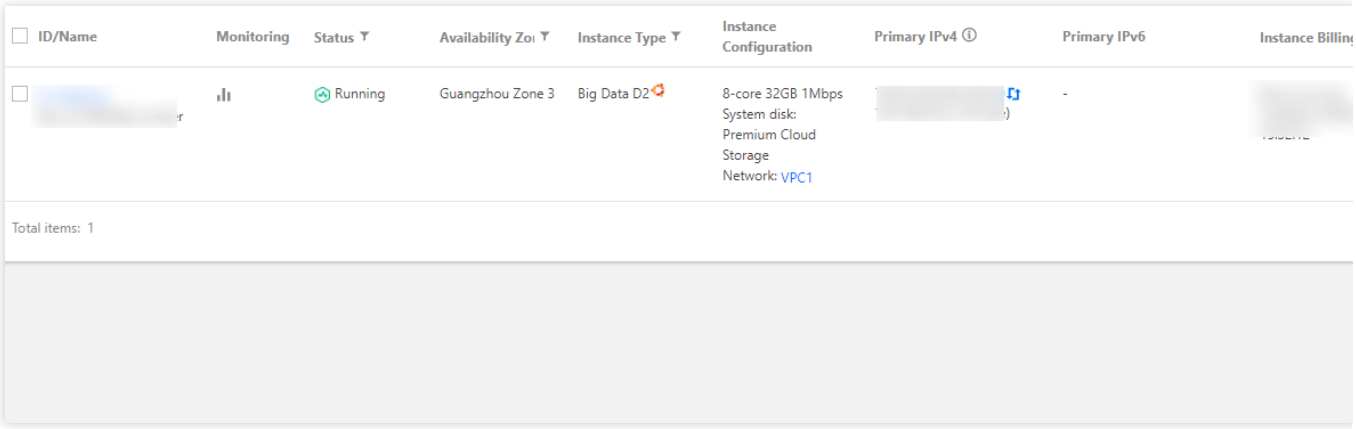
Instal ulang sistem melalui Konsol

Instal ulang sistem melalui API

## Menginstal ulang sistem melalui Konsol

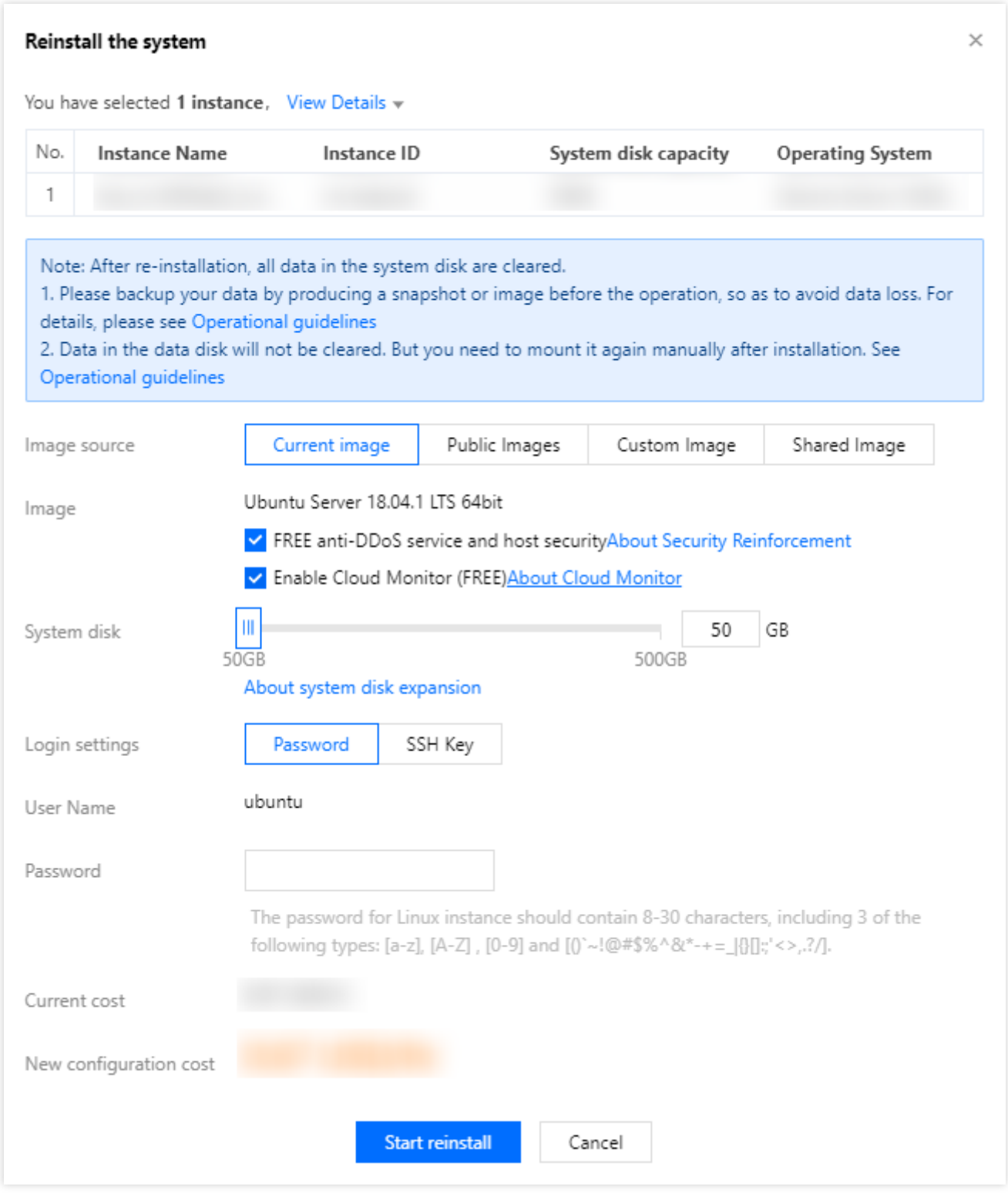
1. Login ke Konsol CVM.

2. Di baris instans yang sistemnya yang ingin Anda instal ulang, klik **More** (Lainnya) > **Reinstall the system** (Instal ulang sistem), seperti yang ditunjukkan pada gambar berikut:




3. Di jendela pop-up yang muncul, klik **OK, reinstall now** (OKE, instal ulang sekarang).

4. Pilih citra yang digunakan oleh instans saat ini atau citra lain, atur ukuran disk, atur kata sandi login untuk instans, lalu klik **Start reinstall** (Mulai instal ulang).




### Menginstal ulang sistem melalui API

Untuk informasi selengkapnya, lihat ResetInstance API.

# Operasi Selanjutnya

Jika CVM Anda telah memasang disk data sebelum penginstalan ulang lintas sistem, lihat dokumen berikut tentang cara membaca data dari disk data sistem operasi asli:

Membaca/Menulis Disk Data EXT setelah Menginstal Ulang CVM Linux ke CVM Windows

Membaca/Menulis Disk Data NTFS setelah Menginstal Ulang CVM Windows ke CVM Linux

# Kepemilikan Kembali Instans

Waktu update terbaru：2021-12-13 17:07:07

Dokumen ini menjelaskan cara memulihkan instans Cloud Virtual Machine (CVM) dari keranjang sampah. Untuk informasi selengkapnya, lihat Pembayaran Jatuh Tempo.

## Keranjang Sampah

Keranjang sampah Tencent Cloud menyediakan mekanisme kepemilikan kembali instans CVM sebagai berikut:
**Pay-as-you-go instances** (Instans bayar sesuai pemakaian): instans bayar sesuai pemakaian akan memasuki keranjang sampah setelah dihentikan oleh pengguna atau pada waktu yang dijadwalkan. Jika akun lewat jatuh tempo, instans bayar sesuai pemakaian tidak akan masuk ke keranjang sampah. Ini akan dirilis setelah akun telah jatuh tempo selama 2 jam dan 15 hari.

### Instans bayar sesuai pemakaian di keranjang sampah

**Retention period** (Periode retensi): instans yang dihentikan oleh pengguna akan disimpan di keranjang sampah selama 2 jam.
**Expiry processing** (Pemrosesan kedaluwarsa): jika instans tidak diperpanjang sebelum periode retensi berakhir, sistem akan melepaskan sumber daya instans dan secara otomatis mengakhiri instans, yang tidak dapat dipulihkan. IP elastis yang terikat pada instans ini juga dirilis.
**Mounting relationship** (Hubungan pemasangan): setelah instans memasuki keranjang sampah, hubungan pemasangannya dengan Cloud Load Balancer, Cloud Block Storage, dan Classiclink **not be automatically terminated** (tidak akan dihentikan secara otomatis).
**Operation restriction** (Pembatasan operasi): instans di keranjang sampah hanya dapat dipulihkan setelah pembaruan atau dihentikan. Beberapa jenis instans mendukung membuat citra kustom
**Perhatian:**
Anda tidak dapat memulihkan instans bayar sesuai pemakaian dari keranjang sampah jika akun Anda lewat jatuh tempo. Harap perbarui pembayaran terlebih dahulu.
Instans bayar sesuai pemakaian disimpan di keranjang sampah selama maksimal 2 jam. Harap perhatikan waktu rilis dan perbarui pembayaran tepat waktu untuk memulihkan instans.
Instans bayar sesuai pemakaian tidak dapat masuk ke keranjang sampah jika akun Anda jatuh tempo. Anda dapat melihatnya di halaman daftar instans CVM. Instans akan dirilis setelah akun Anda jatuh tempo selama 2 jam dan 15 hari.

## Memulihkan Instans

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Recycle Bin** (Keranjang Sampah) -> **Instance Recycle Bin** (Keranjang Sampah Instans) untuk masuk ke daftar daur ulang CVM.
3. Pulihkan satu instans: temukan instans yang akan dipulihkan dalam daftar, klik **Recover** (Pulihkan) di kolom **Operation** (Operasi), dan selesaikan pembayaran perpanjangan.
4. Pulihkan instans dalam kumpulan: pilih semua instans yang akan dipulihkan, klik **Recover Selected** (Pulihkan Instans yang Dipilih) di bagian atas, dan selesaikan pembayaran perpanjangan.

# Instans Spot

Waktu update terbaru：2022-04-14 18:45:11

## Skenario

Dokumen ini memberikan panduan tentang pengelolaan dan pembelian instans spot. Saat ini, instans spot tersedia melalui saluran berikut:
**CVM console** (Konsol CVM): **Spot Instances** (Instans Spot) telah ditambahkan sebagai opsi untuk **Billing Mode** (Mode Penagihan) di halaman pembelian CVM.
**BatchCompute console** (Konsol BatchCompute): Instans spot dapat dipilih saat pengguna mengirimkan pekerjaan dan membuat lingkungan komputasi di konsol BatchCompute.
**TencentCloud API** (TencentCloud API): Parameter yang terkait dengan instans spot telah ditambahkan ke RunInstances API.

## Petunjuk

### Konsol CVM

1. Login ke halaman pembelian CVM.
2. Pada halaman tab **Select a model** (Pilih model), atur **Billing Mode** (Mode Penagihan) ke **Spot Instances** (Instans Spot).
3. Tentukan **Region** (Wilayah), **Availability Zone** (Zona Ketersediaan), **Network** (Jaringan), **Instance** (Instans), dan konfigurasi lainnya seperti yang diperlukan dan diminta.
4. Periksa informasi instans spot yang akan dibeli dan detail biaya setiap item konfigurasi.
5. Klik **Purchase** (Beli) dan selesaikan pembayaran.
Setelah menyelesaikan pembayaran, Anda dapat login ke konsol CVM untuk memeriksa instans spot Anda.

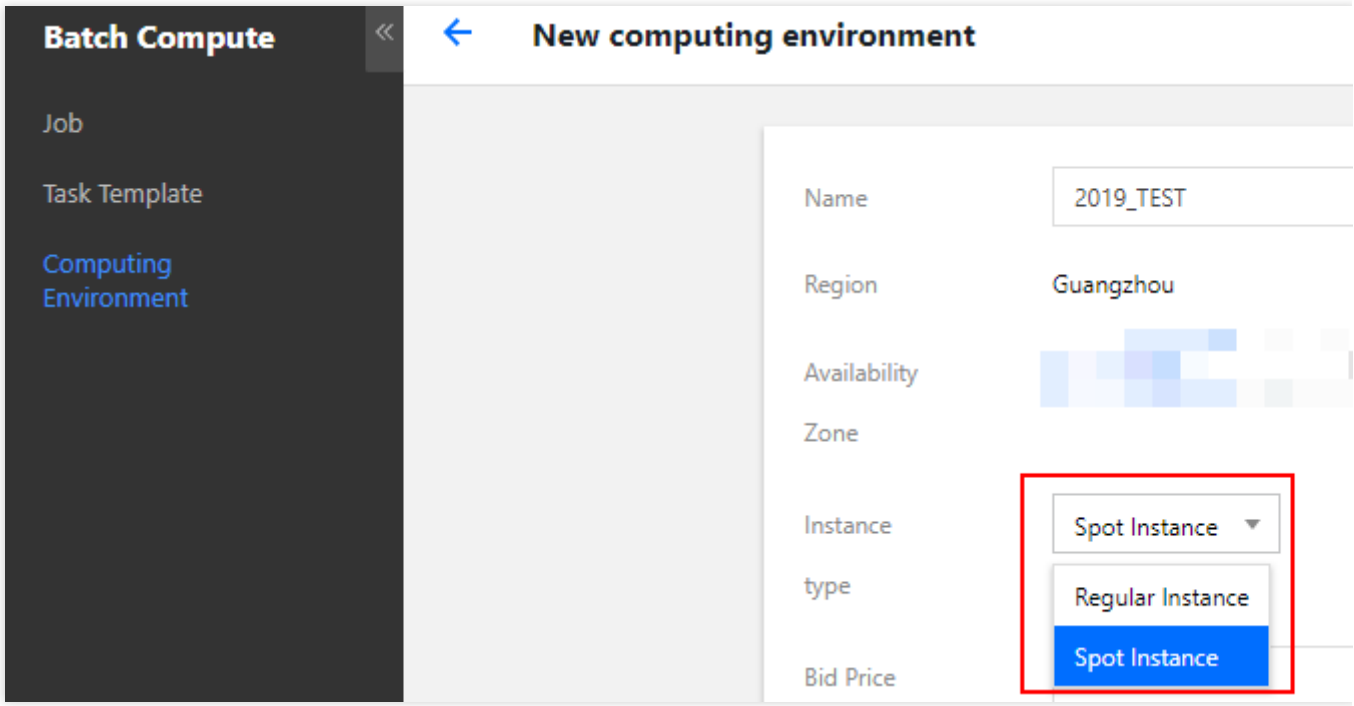
### Konsol BatchCompute

**Async API** (Async API): Ketika Anda mengirimkan pekerjaan, buat lingkungan komputasi, atau modifikasi jumlah instans yang diharapkan dalam lingkungan komputasi, instans BatchCompute akan memproses permintaan Anda secara asinkron. Ketika tidak dapat memenuhi permintaan saat ini karena alasan inventaris atau harga, instans BatchCompute terus menerapkan sumber daya instans spot hingga permintaan saat ini terpenuhi.
Jika Anda perlu merilis instans, Anda perlu menyesuaikan jumlah instans yang diharapkan di lingkungan komputasi melalui konsol BatchCompute. Jika Anda merilis instans melalui konsol CVM, konsol BatchCompute akan secara otomatis membuat instans hingga jumlah instans yang diharapkan terpenuhi.

**Cluster Mode** (Mode Kluster): Lingkungan komputasi instans BatchCompute dapat mempertahankan sekumpulan instans spot sebagai kluster. Anda hanya perlu mengirimkan jumlah yang diharapkan, konfigurasi, dan harga maksimum instans spot. Lingkungan komputasi akan terus berlaku untuk instans spot hingga jumlah yang diharapkan terpenuhi. Meskipun instans spot tidak tersambung ke internet, lingkungan komputasi akan secara otomatis menerapkan instans spot lagi untuk memenuhi jumlah yang diharapkan.
**Fixed Price** (Harga Tetap): Saat ini, instans spot disediakan dengan diskon tetap. Anda harus menetapkan nilai yang lebih besar atau sama dengan harga pasar saat ini. Untuk harga pasar, lihat Instans Spot - Wilayah yang didukung dan jenis instans.

**Petunjuk**

1. Login ke konsol BatchCompute.
2. Pada halaman **Computing environment** (Lingkungan komputasi), pilih wilayah secara acak, seperti Guangzhou, lalu klik **New** (Baru).
Halaman **New computing environment** (Lingkungan komputasi baru) akan muncul.
3. Pada halaman **New computing environment** (Lingkungan komputasi baru), atur **Billing Type** (Jenis Penagihan) ke **Spot Instance** (Instans Spot), lalu tentukan konfigurasi seperti **Model Type** (Jenis Model), **Image** (Citra), **Name** (Nama), dan **Expected quantity** (Kuantitas yang diharapkan) sesuai kebutuhan, seperti yang ditunjukkan pada gambar berikut:




4. Klik **OK** (OKE) untuk menyelesaikan pembuatan.
Kemudian, Anda dapat memeriksa lingkungan komputasi baru di konsol BatchCompute. Untuk melihat kemajuan pembuatan instans CVM yang sedang dibuat di lingkungan komputasi, klik **Activity Logs** (Log Aktivitas) dan **Instance List** (Daftar Instans) untuk lingkungan komputasi.

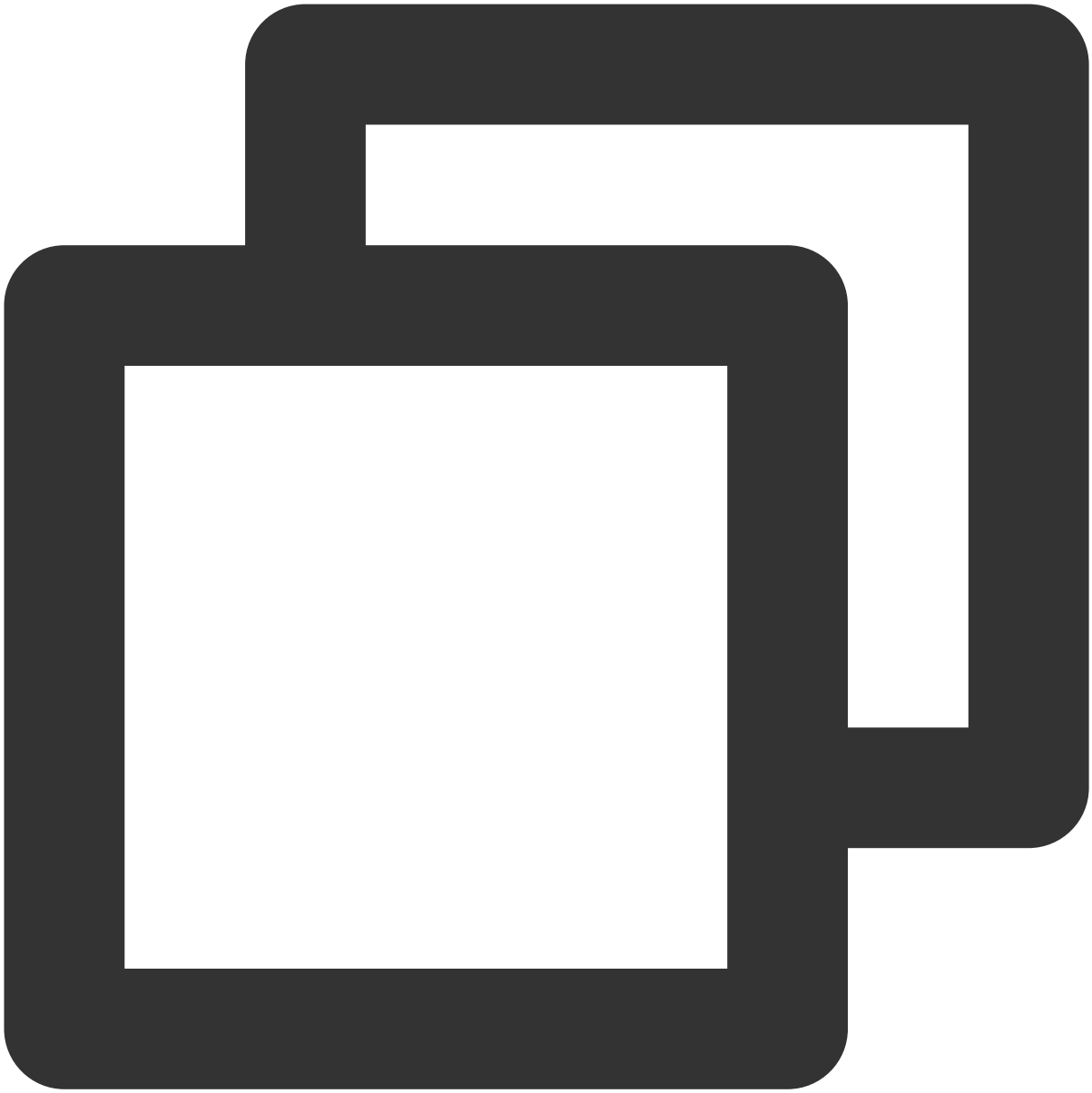
### TencentCloud API

Di RunInstances API, Anda dapat menentukan parameter InstanceMarketOptionsRequest untuk mengaktifkan atau menonaktifkan mode instans spot dan mengonfigurasi informasi tentang instans spot.
**Sync API** (Sync API): Saat ini, RunInstances menyediakan API permintaan sinkronisasi satu kali. Ini berarti bahwa jika aplikasi gagal karena inventaris tidak mencukupi atau harga yang diminta lebih rendah dari harga pasar, RunInstances API segera mengembalikan kode kegagalan dan tidak berlaku untuk instans spot lagi.
**Fixed Price** (Harga Tetap): Saat ini, instans spot disediakan dengan diskon tetap. Anda harus menetapkan nilai yang lebih besar atau sama dengan harga pasar saat ini. Untuk harga pasar, lihat Instans Spot - Wilayah yang didukung dan jenis instans.

#### Contoh

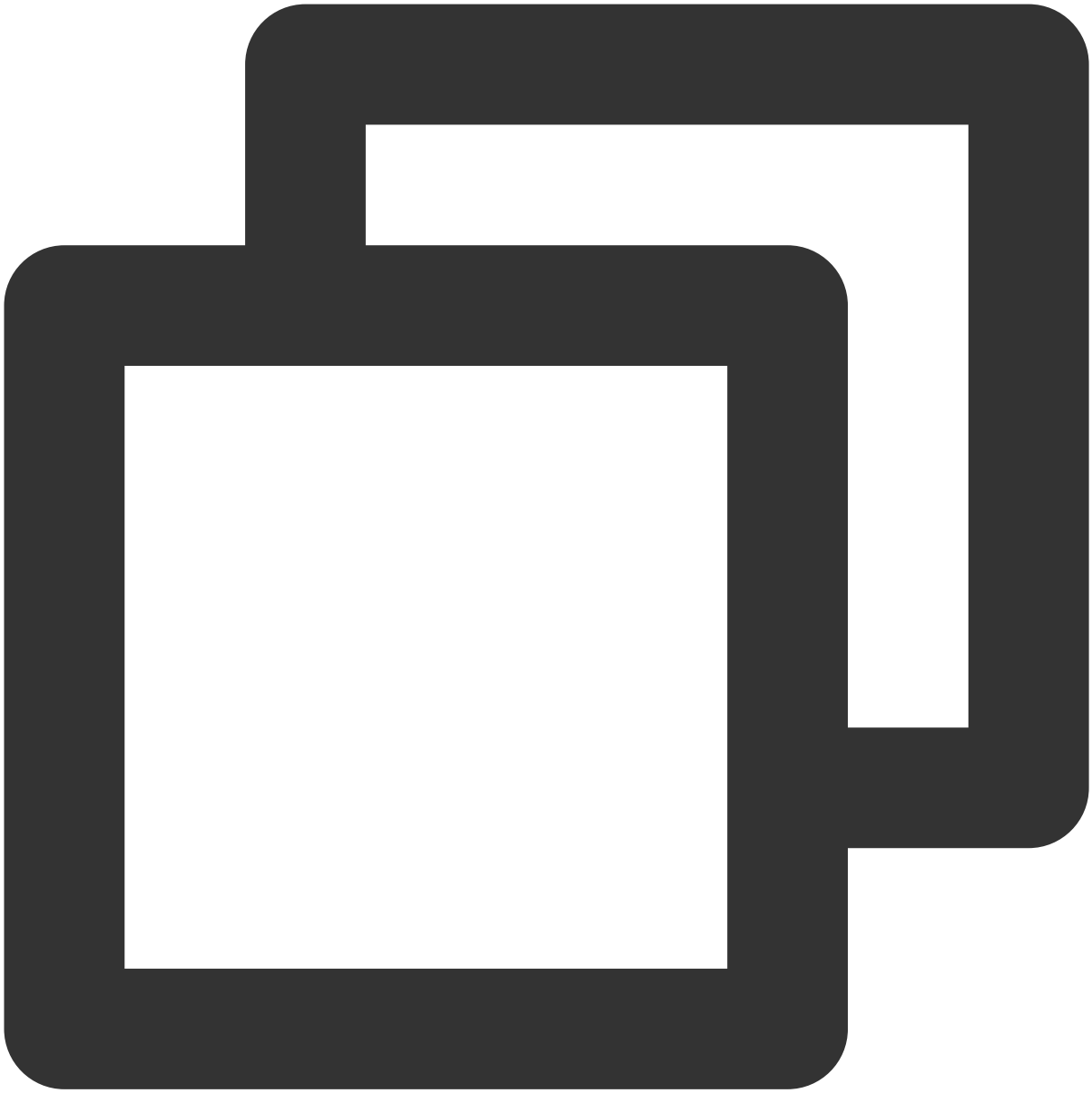
Anda memiliki instans di Zona 3 Guangzhou, dan mode penagihan instans adalah bayar sesuai pemakaian per jam dan dalam mode spot. Konfigurasi spesifik dari mode penagihan adalah sebagai berikut:
MaxPrice: 0,0923 USD/jam
SpotInstanceType: one-time
ImageId: img-pmqg1cw7
InstanceType: S2.MEDIUM4 (Standard 2, 2-core, 4GB)
InstanceCount: 1

#### Meminta parameter



```
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Placement.Zone=ap-guangzhou-3
&InstanceChargeType=SPOTPAID
&InstanceMarketOptions.MarketType=spot
&InstanceMarketOptions.SpotOptions.MaxPrice=0.0923
&InstanceMarketOptions.SpotOptions.SpotInstanceType=one-time
&ImageId=img-pmqg1cw7
&InstanceType=S2.MEDIUM4
&InstanceCount=1
&<common request parameters>
```

**Parameter respons**



```
{
  "Response": {
    "InstanceIdSet": [
      "ins-1vogaxgk"
    ],
    "RequestID": "3c140219-cfe9-470e-b241-907877d6fb03"
  }
}
```

# Mengkueri Status Kepemilikan Kembali dari Instans Spot

Waktu update terbaru：2021-12-13 17:07:05

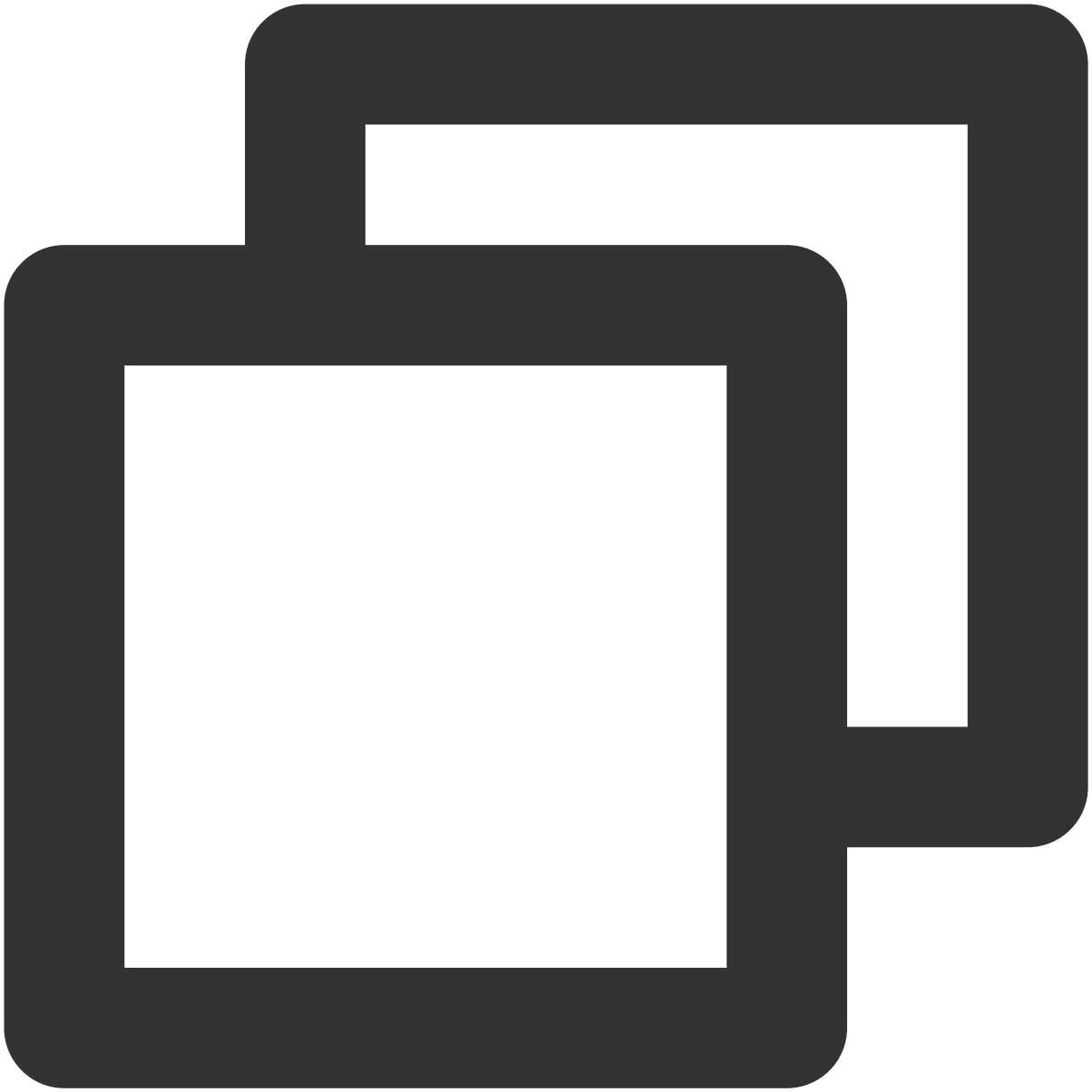
Instans spot dapat diambil alih oleh Tencent Cloud karena alasan harga atau inventaris. Untuk memungkinkan pengguna melakukan operasi kustom sebelum kepemilikan kembali instans, kami menyediakan API untuk memperoleh informasi tentang status kepemilikan kembali melalui mekanisme metadata internal.

## Metadata

Metadata instans mengacu pada data yang relevan dengan sebuah instans. Metadata ini dapat digunakan untuk mengonfigurasi atau mengelola instans operasi. Anda dapat mengakses dan mendapatkan metadata instans melalui sebuah instans. Untuk informasi selengkapnya, lihat Metadata Instans.

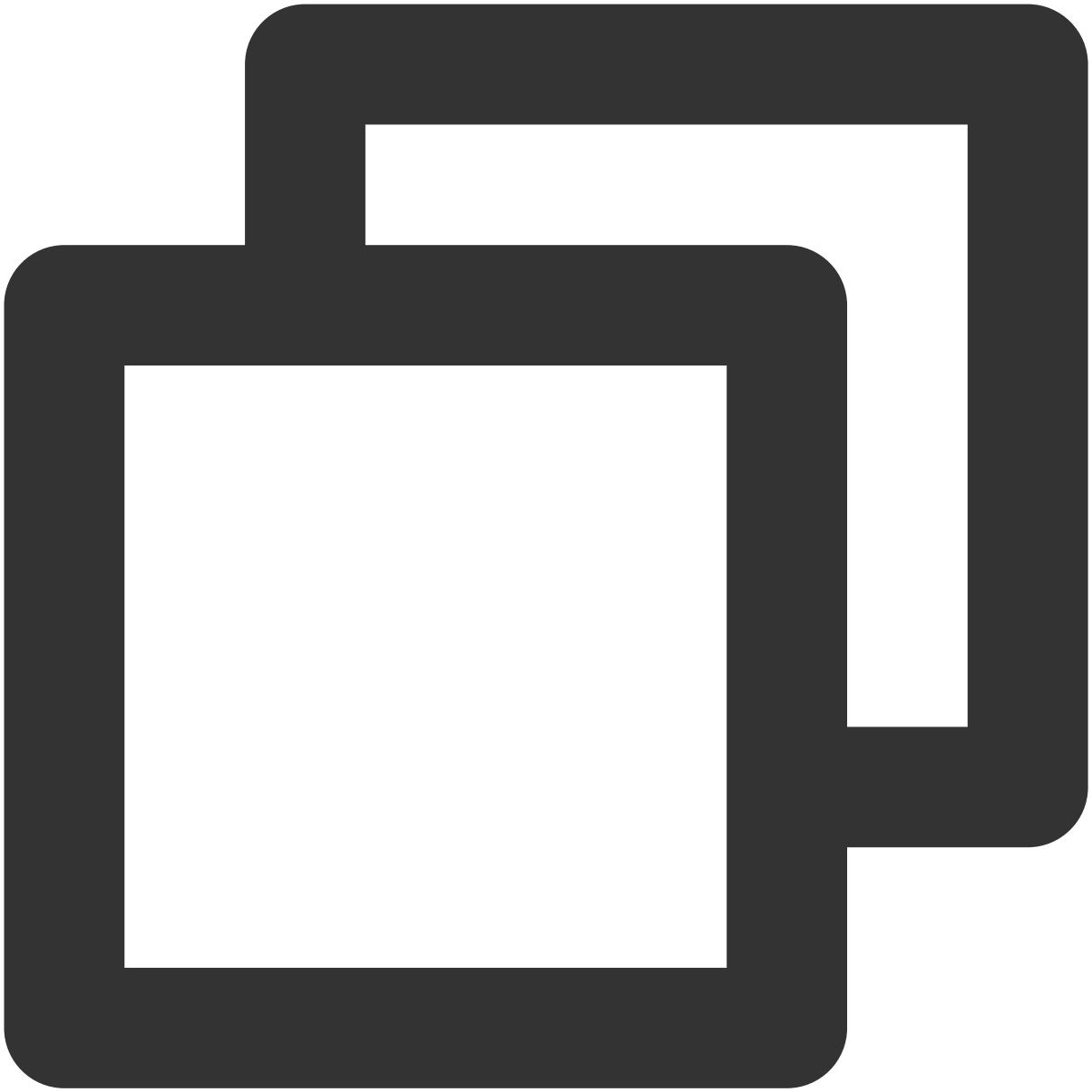
## Menggunakan metadata untuk mendapatkan informasi tentang status kepemilikan kembali instans spot

Untuk mendapatkan informasi tentang status kepemilikan kembali instans spot, Anda dapat mengakses metadata dengan menggunakan alat cURL atau permintaan HTTP GET.



```
curl metadata.tencentyun.com/latest/meta-data/spot/termination-time
```

Jika informasi berikut ditampilkan, hal ini menunjukkan waktu kepemilikan kembali instans spot.



```
2018-08-18 12:05:33
```

Jika kode kesalahan 404 ditampilkan, artinya instans bukan instans spot atau kepemilikan kembali belum dipicu.

Untuk informasi selengkapnya, lihat Metadata Instans.

# Tidak Ada Biaya Saat Mematikan Instans Pembayaran Sesuai Pemakaian

Waktu update terbaru：2021-12-13 17:07:08

## Ikhtisar

Jika Anda mengaktifkan "Tanpa Biaya saat Pematian" saat menonaktifkan instans bayar sesuai pemakaian, penagihan sumber daya CPU dan memori instans ini akan berhenti. Namun, disk Cloud (disk sistem dan disk data), bandwidth jaringan publik, citra, dan komponen utama lainnya dari instans CVM dikenakan biaya.

**Perhatian:**

Saat fitur ini diaktifkan, sumber daya CPU dan memori instans **will not be retained** (tidak akan dipertahankan), dan alamat IP publik **will be automatically released** (akan dirilis secara otomatis) setelah dinonaktifkan. Untuk informasi selengkapnya tentang fitur, batas penggunaannya, dan dampaknya, lihat Tanpa Biaya Saat Pematian untuk Instans Bayar Sesuai Pemakaian.

## Petunjuk

### Mematikan instans melalui konsol

1. Login ke konsol CVM.
2. Pilih metode operasi yang sesuai berdasarkan kebutuhan Anda yang sebenarnya.

Mematikan satu instans:

2.1.1 Pilih instans yang ingin dimatikan, lalu klik **More** (Lainnya) > **Instance Status** (Status Instans) > **Shut down** (Matikan) di bawah kolom **Operation** (Operasi) di sebelah kanan.

2.1.2 Centang **CVM No Charge when Shut down** (CVM Tanpa Biaya saat Pematian), lalu klik **OK** (OKE).

Jika instans tidak mendukung fitur ini, **"No Charge when Shut Down" is not supported** (("CVM Tanpa Biaya saat Mematikan" tidak didukung)) akan ditampilkan dalam daftar instans.

Mematikan beberapa instans:

2.1.1 Pilih semua instans yang ingin Anda matikan, lalu klik **Shut down** (Matikan) di bagian atas daftar untuk mematikan instans dalam batch.

Alasan diberikan untuk instans yang tidak dapat dionaktifkan.

2.1.2 Centang **CVM No Charge when Shut down** (CVM Tanpa Biaya saat Pematian), lalu klik **OK** (OKE).

Jika instans tidak mendukung fitur ini, **"No Charge when Shut Down" is not supported** (("CVM Tanpa Biaya saat Mematikan" tidak didukung)) akan ditampilkan dalam daftar instans.

### Mematikan instans melalui API

Anda dapat menggunakan `StopInstances` API untuk mematikan instans. Untuk detailnya, harap lihat StopInstances. Untuk mengaktifkan fitur ini melalui API, tambahkan parameter berikut:

| Nama Parameter | Wajib | Jenis | Deskripsi |
| --- | --- | --- | --- |
| Mode Berhenti | Tidak | String | Fitur "Tanpa Biaya saat Pematian" hanya tersedia untuk instans bayar sesuai pemakaian.<br>**Valid values:** (Nilai yang valid:)<br>KEEP_CHARGING: instans dikenakan biaya setelah pematian<br>STOP_CHARGING: tanpa biaya saat pematian<br>**Default value:** (Nilai default:)<br>KEEP_CHARGING |

# Citra
# Membuat Citra Kustom

Waktu update terbaru：2024-05-16 11:09:47

## Ikhtisar

Selain menggunakan citra publik Tencent Cloud, Anda dapat membuat citra kustom untuk membuat dengan cepat instans Tencent Cloud CVM dengan konfigurasi yang sama.

**Keterangan:**

Citra menggunakan layanan snapshot CBS untuk penyimpanan data. Saat Anda membuat citra kustom, snapshot akan dibuat secara otomatis dan dikaitkan dengan citra tersebut. Anda akan dikenakan biaya untuk snapshot ini. Untuk informasi selengkapnya, lihat Ikhtisar Penagihan.

Untuk CVM yang dibuat berdasarkan citra publik setelah Juli 2018 dan menggunakan disk cloud sebagai disk sistem, Anda dapat membuat citra tanpa menonaktifkan instans. Untuk CVM lain, Anda harus mematikan instans sebelum membuat citra kustom untuk memastikan bahwa citra memiliki lingkungan deployment yang sama dengan instans saat ini.

## Catatan

Setiap wilayah mendukung maksimal 500 citra kustom.

Direktori dan file berikut akan dihapus.

`/var/log/`

`/root/.bash_history` dan `/home/ubuntu/.bash_history` (untuk sistem operasi Ubuntu)

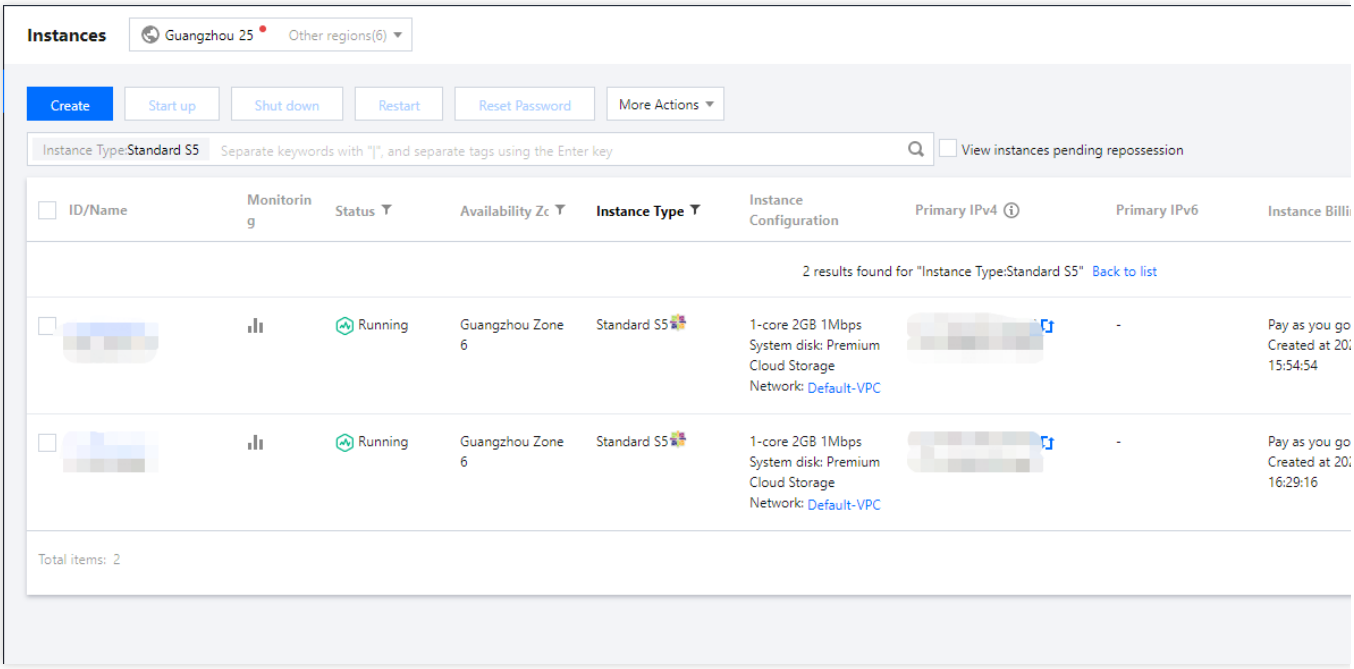
Saat membuat citra kustom pada instans Linux, pastikan `/etc/fstab` tidak berisi konfigurasi disk data. Jika tidak, instans yang dibuat dengan citra ini tidak dapat dimulai secara normal. Jika instans Linux yang digunakan untuk membuat citra kustom memiliki disk data yang terpasang, beri komentar atau hapus konfigurasi disk data yang relevan di `/etc/fstab` .

Proses pembuatan memakan waktu sepuluh menit atau lebih, tergantung pada ukuran data instans. Harap persiapkan terlebih dahulu untuk menghindari dampak bisnis.

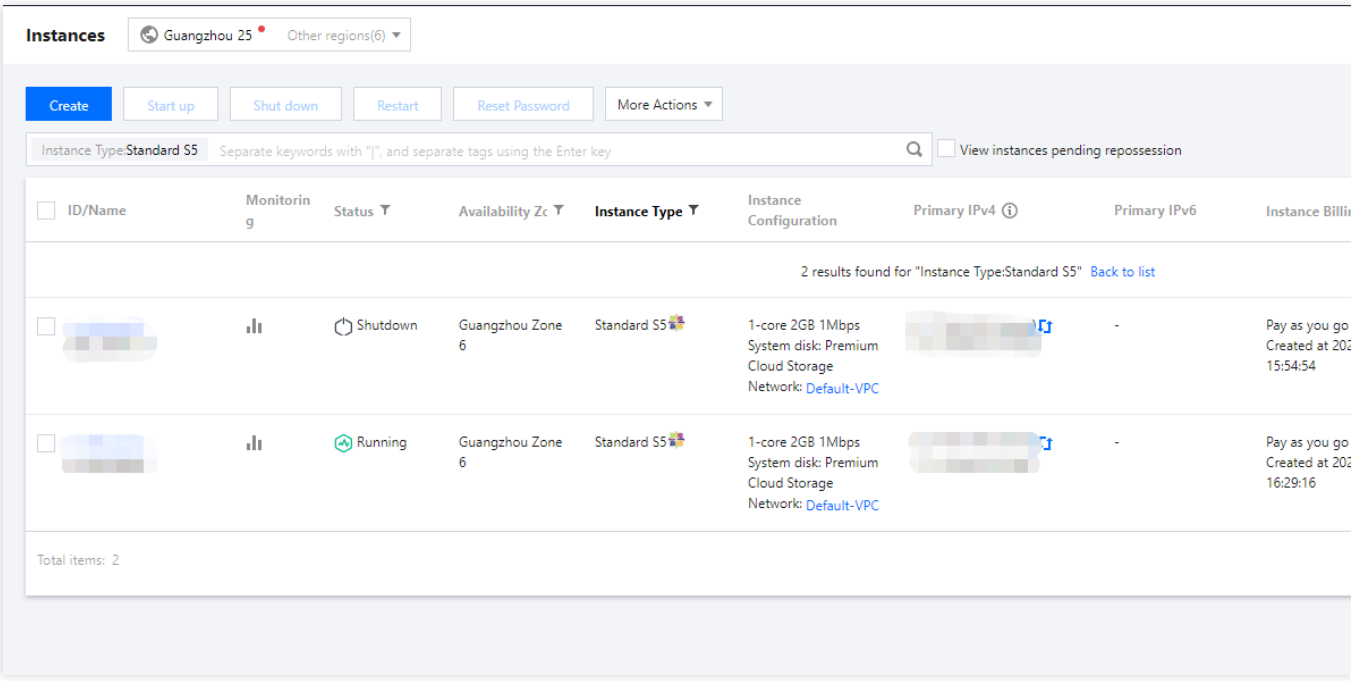
## Petunjuk

### Membuat citra kustom dari instans melalui konsol

1. Login ke konsol CVM.
2. Pada halaman manajemen instans, pilih instans untuk citra yang akan dibuat, lalu klik **More** (Lainnya) > **Instance Status** (Status Instans) > **Shut down** (Nonaktifkan), seperti yang ditunjukkan di bawah ini:




3. Setelah instans dinonaktifkan, klik **More** (Lainnya)> **Create Image** (Buat Citra), seperti yang ditunjukkan di bawah ini:



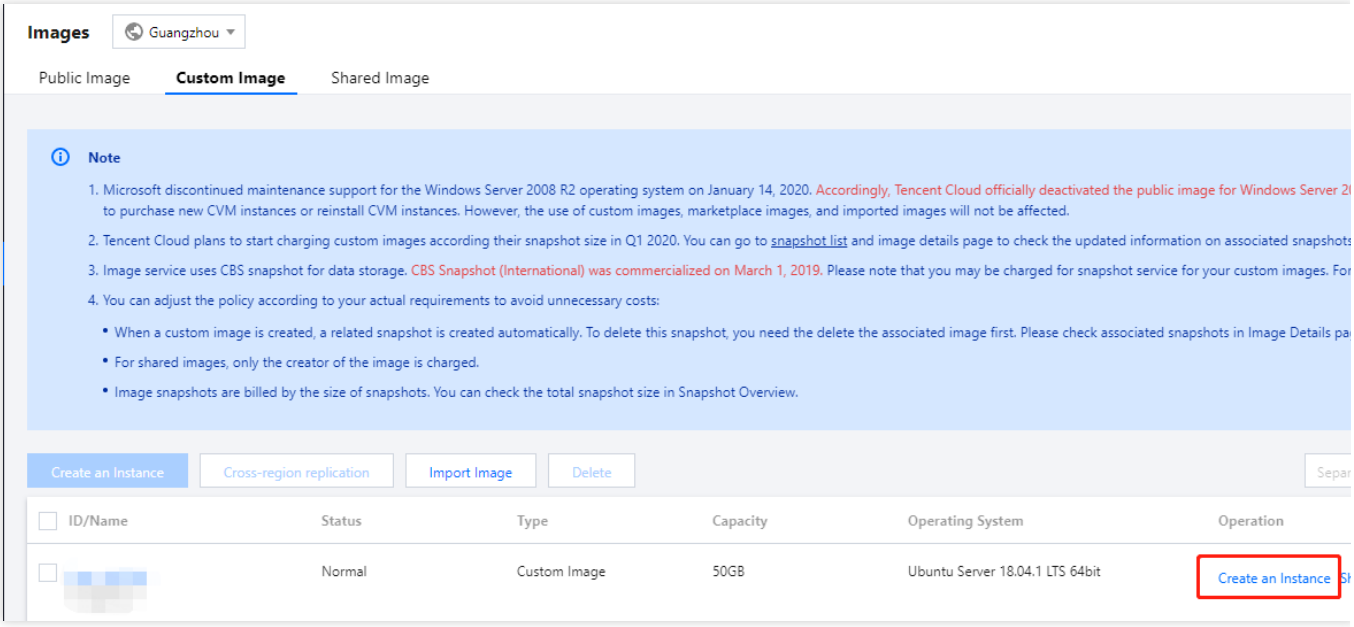

4. Di jendela pop-up, masukkan **Image Name** (Nama Citra) dan **Description** (Deskripsi), lalu klik **Create Image** (Buat Citra).

**Keterangan:**

Anda dapat mengklik

di sudut kanan atas untuk melihat kemajuan pembuatan citra.

5. Setelah citra dibuat, klik **Images** [Citra] di bilah sisi kiri untuk masuk ke halaman manajemen citra.
6. Dalam daftar citra, pilih citra yang telah Anda buat, lalu klik **Create an Instance** (Buat Instans) untuk membeli server dengan konfigurasi yang sama seperti citra.




### Membuat citra kustom melalui API

Anda dapat menggunakan `CreateImage` API untuk membuat citra kustom. Untuk informasi selengkapnya, lihat CreateImage.

# Praktik Terbaik

### Memigrasikan data pada disk data

Jika Anda perlu menyimpan data pada disk data instans asli saat meluncurkan instans baru, Anda dapat mengambil snapshot disk data terlebih dahulu, lalu menggunakan snapshot ini untuk membuat data cloud baru disk.
Untuk informasi selengkapnya, lihat Membuat Disk Cloud Menggunakan Snapshot.

# Membagikan Citra Kustom

Waktu update terbaru：2024-05-16 10:54:13

## Ikhtisar

**Shared image** (Citra yang dibagikan) berarti Anda berbagi dengan **others users** (pengguna lain) **custom image** (citra kustom) yang telah Anda buat. Anda juga dapat memperoleh citra yang dibagikan oleh pengguna lain, mendapatkan komponen yang diperlukan, dan menambahkan konten kustom.

**Perhatian:**

Tencent Cloud tidak menjamin integritas atau keamanan citra yang dibagikan. Harap hanya gunakan citra yang dibagikan dari sumber yang dapat dipercaya.

## Catatan

Setiap citra dapat dibagikan kepada maksimal 500 pengguna Tencent Cloud.

Nama dan deskripsi citra yang dibagikan tidak dapat diubah. Komponen tersebut hanya digunakan untuk membuat instans CVM.

Citra yang dibagikan dengan pengguna lain tidak menempati kuota citra Anda sendiri.

Citra kustom yang telah dibagikan dengan orang lain dapat dihapus, asalkan Anda membatalkan berbagi citra terlebih dahulu. Untuk informasi selengkapnya, lihat Membatalkan Berbagi Citra. Citra yang dibagikan yang Anda peroleh dari orang lain tidak dapat dihapus.

Citra kustom hanya dapat dibagikan dengan akun di wilayah yang sama dengan akun sumber. Untuk berbagi citra dengan pengguna di wilayah lain, Anda perlu menyalinnya ke wilayah target sebelum berbagi.

Citra yang dibagikan yang Anda peroleh dari orang lain tidak dapat dibagikan dengan pengguna ketiga.

## Petunjuk

### Mendapatkan ID akun root yang ingin Anda bagikan citranya

Citra yang dibagikan Tencent Cloud diidentifikasi oleh ID unik dari akun root yang ingin Anda bagikan citranya. Anda dapat memperoleh ID akun pengguna lain sebagai berikut:

1. Login ke konsol CVM.
2. Klik nama akun di sudut kanan atas dan pilih **Account Information** (Informasi Akun).
3. Lihat dan catat ID akun.
4. Minta pengguna lain untuk mengirimkan ID akun kepada Anda.

## Membagikan citra melalui konsol

1. Login ke konsol CVM.
2. Klik **Images** ([Citra]) di bilah sisi kiri.
3. Klik tab **Custom Image** (Citra Kustom) untuk masuk ke halaman pengelolaan citra kustom.
4. Pilih citra kustom yang ingin Anda bagikan di daftar citra kustom, lalu klik **Share** (Bagikan) di sebelah kanan.
5. Di jendela pop-up **Shared Image** (Citra yang Dibagikan), masukkan ID akun tempat Anda ingin membagikan citra, lalu klik **Share** (Bagikan).
6. Akun lain harus masuk ke konsol CVM, lalu pilih **Images** (Citra) > **Shared Image** (Citra yang Dibagikan) untuk melihat citra yang telah Anda bagikan.
7. Ulangi langkah-langkah di atas untuk membagikan citra dengan beberapa pengguna.

## Membagikan citra melalui API

Anda dapat menggunakan `ShareImage` API untuk membagikan citra. Untuk informasi selengkapnya, lihat `ShareImage` API.

# Membatalkan Berbagi Citra

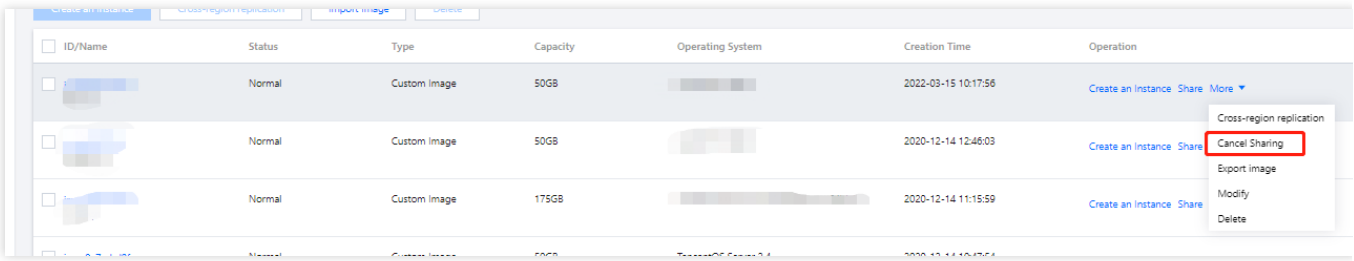
Waktu update terbaru：2022-04-14 15:12:36

## Skenario

Dokumen ini menjelaskan cara membatalkan berbagi citra kustom. Anda dapat membatalkan status berbagi citra dengan pengguna lain kapan saja. Tindakan ini tidak memengaruhi instans yang dibuat oleh pengguna lain yang menggunakan citra yang dibagikan ini, tetapi instans tidak dapat lagi melihat citra atau membuat instans baru menggunakan citra ini.

## Petunjuk

Membatalkan berbagi citra melalui konsol
Membatalkan berbagi citra melalui API
1. Login ke Konsol CVM.Di bilah sisi kiri, klik Images (Citra).
2. Pilih tab **Custom Image** (Citra Kustom) untuk masuk ke halaman pengelolaan citra kustom.
3. Dalam daftar citra kustom, pilih citra kustom yang ingin Anda batalkan berbaginya, lalu klik **More** (Lainnya) > **Cancel Sharing** (Batalkan Berbagi).




4. Di halaman baru, pilih ID unik akun tempat Anda ingin membatalkan berbagi citra dan klik **Cancel Sharing** (Batalkan Berbagi).
5. Di jendela pop-up, klik **OK** (OKE) untuk membatalkan berbagi citra.
Anda dapat menggunakan ModifyImageSharePermission API untuk membatalkan berbagi citra. Untuk informasi selengkapnya, lihat ModifyImageSharePermission.

# Menghapus Citra Kustom

Waktu update terbaru：2022-09-15 11:31:50

## Skenario

Dokumen ini menjelaskan cara menghapus citra kustom.

## Catatan

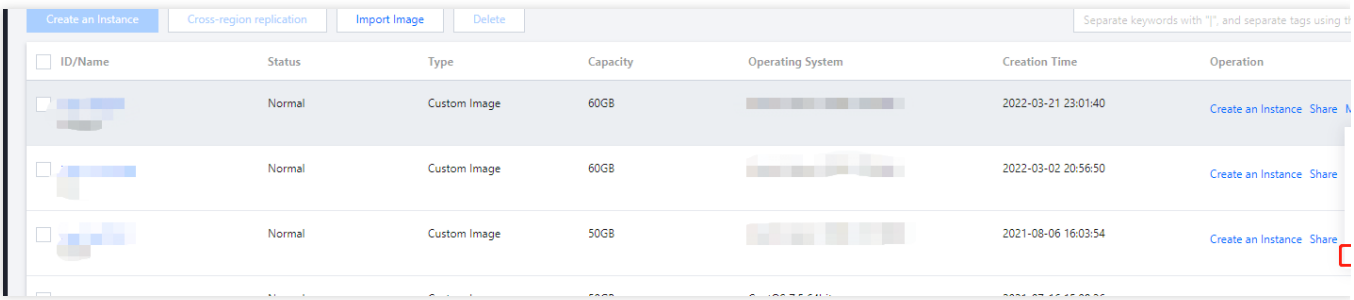
Sebelum menghapus citra kustom, harap perhatikan item berikut:
Setelah citra kustom dihapus, citra tersebut tidak dapat lagi digunakan untuk memulai instans CVM baru, tetapi tidak akan memengaruhi instans yang telah dimulai. Jika Anda ingin menghapus semua instans yang dimulai dari citra ini, lihat Mengklaim Kembali Instans atau Menghentikan Instans.
Citra kustom yang telah dibagikan dengan orang lain tidak dapat dihapus. Untuk menghapusnya, Anda harus membatalkan berbagi citra terlebih dahulu. Untuk informasi selengkapnya, lihat Batalkan Berbagi Citra.
Anda hanya dapat menghapus citra kustom, bukan citra umum atau citra bersama.

## Petunjuk

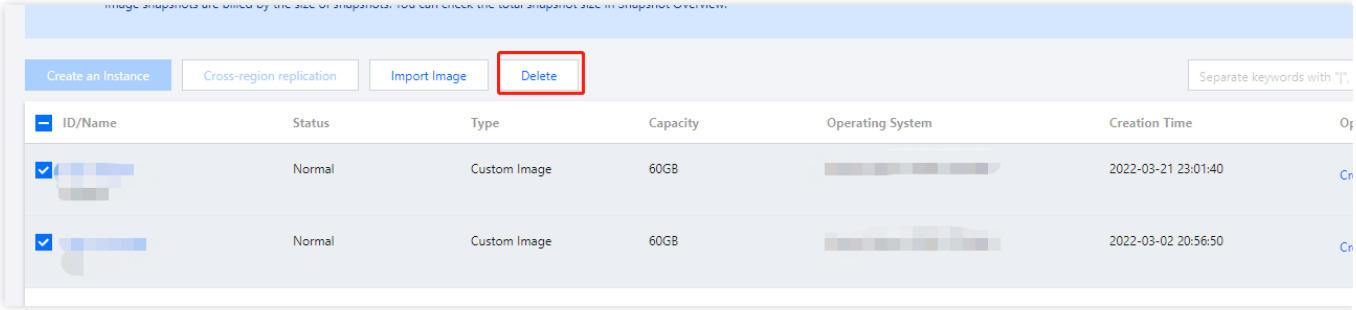
### Hapus citra melalui konsol

1. Login ke Konsol CVM. Di bilah kiri, klik **Images** (Citra)
2. Dan pilih tab **Custom Image** (Citra Kustom) untuk masuk ke halaman manajemen citra kustom.
3. Pilih metode untuk menghapus citra kustom berdasarkan kebutuhan aktual.

**Menghapus satu citra**: cari citra khusus yang akan dihapus dalam daftar citra dan klik **More** (Lainnya) > **Delete** (Hapus).



**Menghapus banyak citra**: pilih semua citra kustom yang akan dihapus dalam daftar citra, lalu klik **Delete** (Hapus) di bagian atas.




4. Di jendela pop-up, klik **OK** (OKE).

Jika penghapusan gagal, kemungkinan akan ditampilkan alasannya.

## Hapus citra melalui API

Anda dapat menggunakan DeleteImages API untuk menghapus citra. Untuk detailnya, lihat Menghapus Citra.

# Menyalin Citra

Waktu update terbaru：2024-01-02 10:12:54

## Ikhtisar

### Langkah-Langkah Umum

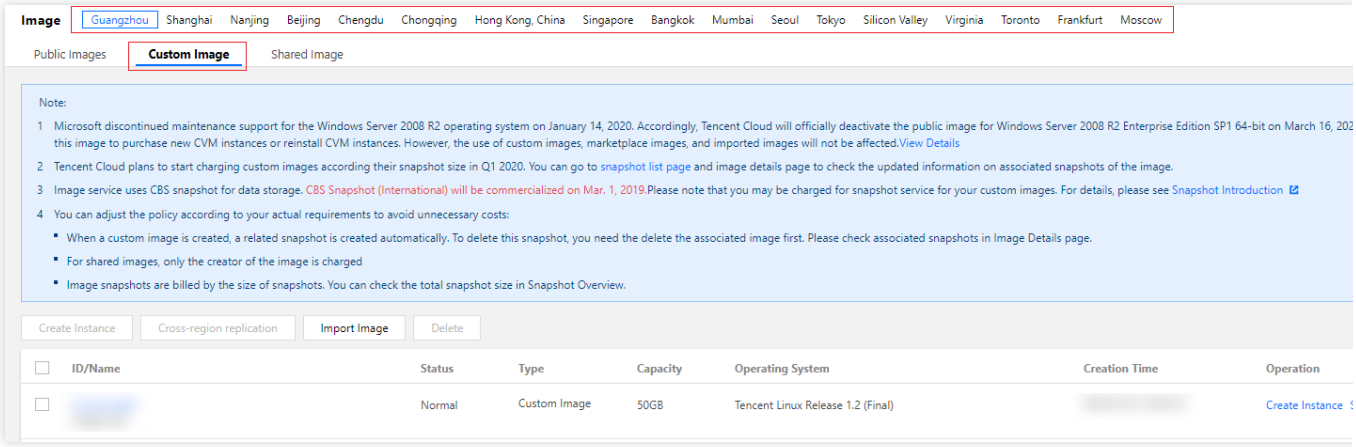
**Cross-region replication** (Replikasi lintas-wilayah) dapat membantu pengguna men-deploy CVM yang sama **across regions** (di seluruh wilayah) dengan cepat. Anda dapat menggunakan fitur ini untuk menyalin citra di seluruh wilayah, lalu membuat CVM dengan menyalin citra di bawah wilayah baru.

### Catatan

Citra yang disalin harus berupa citra kustom. Anda harus membuat citra kustom terlebih dahulu. Untuk detailnya, lihat Membuat Citra Kustom.
Replikasi lintas wilayah memungkinkan Anda menyalin citra di dalam atau di luar Tiongkok. Jika Anda perlu menyalin citra dari Tiongkok ke negara lain atau sebaliknya, harap hubungi layanan purna jual.
Replikasi citra lintas wilayah saat ini gratis.
Replikasi lintas wilayah saat ini tidak mendukung citra kustom yang lebih besar dari 50 GB.
Replikasi lintas wilayah memerlukan waktu 10 hingga 30 menit.

## Metode

Copy images via console
Copy images via API
1. Login ke Konsol CVM.
2. Di bilah sisi kiri, klik **Images** ([Citra]) untuk masuk ke halaman pengelolaan citra.
3. Pilih wilayah tempat citra asli berada yang ingin Anda salin, dan klik tab **Custom Image** (Citra Kustom), seperti yang ditunjukkan di bawah ini:
Misalnya, pilih wilayah Guangzhou.




4. Temukan instans yang citranya perlu disalin, klik **More** (Lainnya) > **Cross-region replication** (Replikasi lintas wilayah).

**Keterangan:**

Untuk operasi batch, pilih semua citra yang ingin Anda salin, lalu klik **Cross-region replication** (Replikasi lintas wilayah).

5. Di jendela pop-up "Cross-region copying" (Penyalinan lintas wilayah), pilih wilayah tempat citra akan disalin dan klik **OK** (OKE).

Setelah penyalinan selesai, daftar citra di wilayah tujuan akan menampilkan citra dengan nama yang sama dan ID yang berbeda.

6. Beralih ke wilayah tujuan. Pilih citra yang berhasil disalin dalam daftar citra di bawah wilayah, lalu klik **Create Instance** (Buat Instans) untuk membuat instans CVM yang sama.

Anda juga dapat menggunakan SyncCvmImage API untuk menyalin citra.

# Impor Citra

## Ikhtisar

Waktu update terbaru：2024-01-02 10:16:43

Selain membuat citra kustom, Tencent Cloud memungkinkan Anda mengimpor citra. Anda dapat mengimpor file citra dari disk sistem di server lokal atau lainnya ke dalam citra kustom CVM. Anda dapat menggunakan citra yang diimpor untuk membuat CVM atau menginstal ulang sistem operasi untuk CVM yang ada.

## Persiapan

Siapkan file citra yang memenuhi persyaratan impor.

**Requirements for Linux images:** (Persyaratan untuk citra Linux:)

| Atribut Citra | Persyaratan |
| --- | --- |
| OS | CentOS, Ubuntu, Debian, CoreOS, OpenSUSE, dan SUSE.<br>OS 32-bit dan 64-bit didukung. |
| Format citra | RAW, VHD, QCOW2, dan VMDK<br>Jalankan `qemu-img info imageName \| grep 'file format'` untuk memeriksa format citra. |
| Jenis sistem file | Partisi GPT tidak didukung. |
| Ukuran citra | Ukuran citra sebenarnya tidak boleh melebihi 50 GB. Jalankan `qemu-img info imageName \| grep 'disk size'` untuk memeriksa ukuran citra.<br>Ukuran citra tidak boleh melebihi 500 GB. Jalankan `qemu-img info imageName \| grep 'virtual size'` untuk memeriksa ukuran citra.<br>**Catatan**: ukuran citra dalam format QCOW2 digunakan saat pemeriksaan selama impor. |
| Jaringan | Secara default, Tencent Cloud menyediakan antarmuka jaringan `eth0` untuk instans.<br>Anda dapat menggunakan metadata layanan untuk mengkueri konfigurasi jaringan instans. Untuk informasi selengkapnya, lihat Metadata Instans. |
| Driver | Driver virtio dari modul virtualisasi KVM harus diinstal untuk satu citra. Untuk informasi selengkapnya, lihat Memeriksa Driver Virtio di Linux.<br>Sebaiknya menginstal cloud-init untuk citra tersebut. Untuk informasi selengkapnya, lihat Menginstal Cloud-Init di Linux. |

| | |
|---|---|
| | Jika cloud-init tidak dapat diinstal, konfigurasikan instans dengan melihat Mengimpor Citra Secara Paksa. |
| Kernel | Kernel native lebih disarankan untuk citra. Modifikasi apa pun pada kernel dapat menyebabkan kegagalan impor. |
| Wilayah | Mengimpor citra dari COS di wilayah lain tidak tersedia untuk Shanghai Finance dan Shenzhen Finance. |

**Requirements for Windows images:** (Persyaratan untuk citra Windows:)

| Atribut Citra | Persyaratan |
|---|---|
| OS | Versi terkait Windows Server 2008, Windows Server 2012, dan Windows Server 2016<br>OS 32-bit dan 64-bit didukung. |
| Format citra | RAW, VHD, QCOW2, dan VMDK<br>Jalankan `qemu-img info imageName \| grep 'file format'` untuk memeriksa format citra. |
| Jenis sistem file | Hanya NTFS dengan partisi MBR yang didukung.<br>Partisi GPT tidak didukung.<br>Logical Volume Manager (LVM) tidak didukung. |
| Ukuran citra | Ukuran citra sebenarnya tidak boleh melebihi 50 GB. Jalankan `qemu-img info imageName \| grep 'disk size'` untuk memeriksa ukuran citra.<br>Ukuran citra tidak boleh melebihi 500 GB. Jalankan qemu-img info imageName \| grep 'virtual size' untuk memeriksa ukuran citra.<br>**Catatan**: ukuran citra dalam format QCOW2 digunakan saat pemeriksaan selama impor. |
| Jaringan | Secara default, Tencent Cloud menyediakan antarmuka jaringan `koneksi area lokal` untuk instans.<br>Anda dapat menggunakan layanan metadata untuk mengkueri konfigurasi jaringan instans. Untuk informasi selengkapnya, lihat Metadata Instans. |
| Driver | Driver Virtio dari modul virtualisasi KVM harus diinstal untuk satu citra. Sistem Windows tidak dilengkapi dengan driver Virtio secara default, jadi harap menginstal driver Windows Virtio terlebih dahulu sebelum mengekspor citra lokal. Pilih alamat pengunduhan berdasarkan lingkungan jaringan:<br>Alamat pengunduhan Internet:<br>`http://mirrors.tencent.com/install/windows/virtio_64_1.0.9.exe`<br>Alamat pengunduhan jaringan pribadi:<br>`http://mirrors.tencentyun.com/install/windows/virtio_64_1.0.9.exe` |
| Wilayah | Mengimpor citra dari COS di wilayah lain tidak tersedia untuk Shanghai Finance dan Shenzhen Finance. |

| | |
|---|---|
| Lainnya | Citra Windows yang diimpor tidak mendukung aktivasi sistem Windows. |

# Petunjuk

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Images** (Citra).
3. Pilih **Custom Image** (Citra Kustom), lalu klik **Import Image** (Impor Citra).
4. Aktifkan Cloud Object Storage, lalu buat bucket. Unggah file citra ke bucket dan dapatkan URL file citra.
5. Klik **Next** (Selanjutnya).
6. Selesaikan konfigurasi, alu klik **Import** (Impor).

**Perhatian:**

Pastikan URL file COS yang dimasukkan sudah benar.

Anda akan diberi tahu tentang hasil impor melalui konsol Pusat Pesan.

# Impor yang Gagal

Jika pengimporan gagal, pecahkan masalah dengan cara sebagai berikut:

## Catatan

Pastikan Anda telah berlangganan pemberitahuan layanan produk melalui Langganan Pesan. Tindakan ini memastikan Anda dapat menerima pesan internal, pesan SMS, dan email tentang penyebab kegagalan.

**Perhatian:**

Jika Anda tidak berlangganan pemberitahuan layanan produk, Anda tidak akan menerima pesan internal tentang apakah impor berhasil.

## Pemecahan Masalah

Untuk informasi selengkapnya tentang pesan kesalahan dan deskripsi, lihat Kode Kesalahan.

### InvalidUrl: URL COS tidak valid

Kesalahan InvalidUrl menunjukkan bahwa telah memasukkan URL COS yang salah. Kemungkinan penyebabnya adalah:

URL citra yang Anda masukkan bukan URL citra Cloud Object Storage.

Izin URL COS bukan untuk pembacaan publik dan penulisan pribadi.

Izin akses file COS dibaca secara pribadi, tetapi tanda tangannya telah kedaluwarsa.

**Perhatian:**

URL COS dengan tanda tangan hanya dapat diakses satu kali.

URL COS dari wilayah lain telah dimasukkan.

**Perhatian:**

Layanan impor citra mengakses server COS di wilayah lokal melalui jaringan pribadi.

File citra pengguna telah dihapus.

URL COS dengan tanda tangan telah digunakan.

Jika Anda menerima pesan kesalahan tentang URL COS yang tidak valid, pecahkan masalah berdasarkan alasan di atas.

#### InvalidFormatSize: format atau ukuran tidak valid

Kesalahan InvalidFormatSize menunjukkan bahwa format atau ukuran citra yang akan diimpor tidak memenuhi persyaratan Tencent Cloud berikut:

Format file citra yang didukung adalah `qcow2` , `vhd` , `vmdk` , dan `raw` .

Ukuran file citra yang akan diimpor tidak boleh melebihi 50 GB (berdasarkan ukuran dalam format qcow2).

Ukuran disk sistem tempat citra diimpor tidak boleh melebihi 500 GB.

Jika Anda menerima pesan kesalahan bahwa format atau ukuran citra tidak valid:

Ubah file citra menjadi format yang sesuai menurut Pembuatan Citra Linux, kurangi konten citra untuk memenuhi persyaratan ukuran, lalu impor ulang.

Anda juga dapat menggunakan fitur migrasi instans offline untuk memigrasikan instans. Fitur ini mendukung migrasi file citra hingga 500 GB.

#### VirtioNotInstall: Driver Virtio tidak diinstal

Kesalahan VirtioNotInstall menunjukkan bahwa citra yang akan diimpor tidak menginstal driver Virtio. Tencent Cloud menggunakan teknologi virtualisasi KVM dan mengharuskan pengguna untuk menginstal driver Virtio pada citra yang akan diimpor. Kecuali untuk beberapa OS Linux yang disesuaikan, sebagian besar OS Linux telah menginstal driver Virtio. Di OS Windows, pengguna perlu menginstal driver Virtio secara manual:

Untuk impor citra Linux, harap lihat Memeriksa Driver Virtio di Linux.

Untuk impor citra Windows, lihat Pembuatan Citra Windows untuk menginstal driver Virtio.

#### CloudInitNotInstalled: program cloud-init tidak diinstal

Kesalahan CloudInitNotInstalled menunjukkan bahwa citra yang akan diimpor tidak menginstal cloud-init. Tencent Cloud menggunakan perangkat lunak cloud-init sumber terbuka untuk menginisialisasi CVM. Jika cloud-init tidak diinstal, inisialisasi CVM akan gagal.

Untuk impor citra Linux, lihat Menginstal Cloud-Init di Linux.

Untuk impor citra Windows, lihat Menginstal Cloudbase-Init di Windows.

Setelah cloud-init atau cloudbase-init diinstal, ganti file konfigurasi berdasarkan dokumen yang sesuai sehingga CVM dapat menarik data dari sumber data yang benar saat startup.

#### PartitionNotPresent: informasi partisi tidak ditemukan

Kesalahan PartitionNotPresent menunjukkan bahwa citra yang diimpor tidak lengkap. Periksa apakah partisi boot disertakan saat citra dibuat.

**RootPartitionNotFound: partisi root tidak ditemukan**

Kesalahan RootPartitionNotFound menunjukkan bahwa partisi root tidak dapat dideteksi pada citra yang akan diimpor. Periksa file citra. Kemungkinan penyebabnya adalah:
Paket penginstalan telah diunggah.
Citra disk data telah diunggah.
Citra partisi boot telah diunggah.
File yang salah diunggah.

**InternalError: kesalahan yang tidak diketahui**

Kesalahan InternalError menunjukkan bahwa sebab kesalahan belum dicatat. Hubungi layanan pelanggan, kemudian tenaga teknis kami akan membantu Anda mengatasi masalah tersebut.

# Kode Kesalahan

| Kode Kesalahan | Alasan | Solusi yang Direkomendasikan |
|---|---|---|
| InvalidUrl | Tautan COS tidak valid. | Periksa apakah URL COS sama dengan URL citra yang diimpor. |
| InvalidFormatSize | Format atau ukuran tidak memenuhi persyaratan. | Citra harus memenuhi persyaratan `image format` dan `image size` di Persiapan. |
| VirtioNotInstall | Driver Virtio tidak diinstal. | Instal driver Virtio pada citra dengan merujuk ke bagian `Driver` di Persiapan. |
| PartitionNotPresent | Informasi partisi tidak ditemukan. | Citra rusak mungkin karena metode pembuatan citra yang salah. |
| CloudInitNotInstalled | Perangkat lunak cloud-init tidak diinstal. | Instal cloud-init di citra Linux dengan merujuk ke bagian `Driver` di Persiapan. |
| RootPartitionNotFound | Partisi root tidak ditemukan. | Citra rusak mungkin karena metode pembuatan citra yang salah. |
| InternalError | kesalahan lainnya. | Hubungi layanan pelanggan kami. |

# Impor Citra secara Paksa

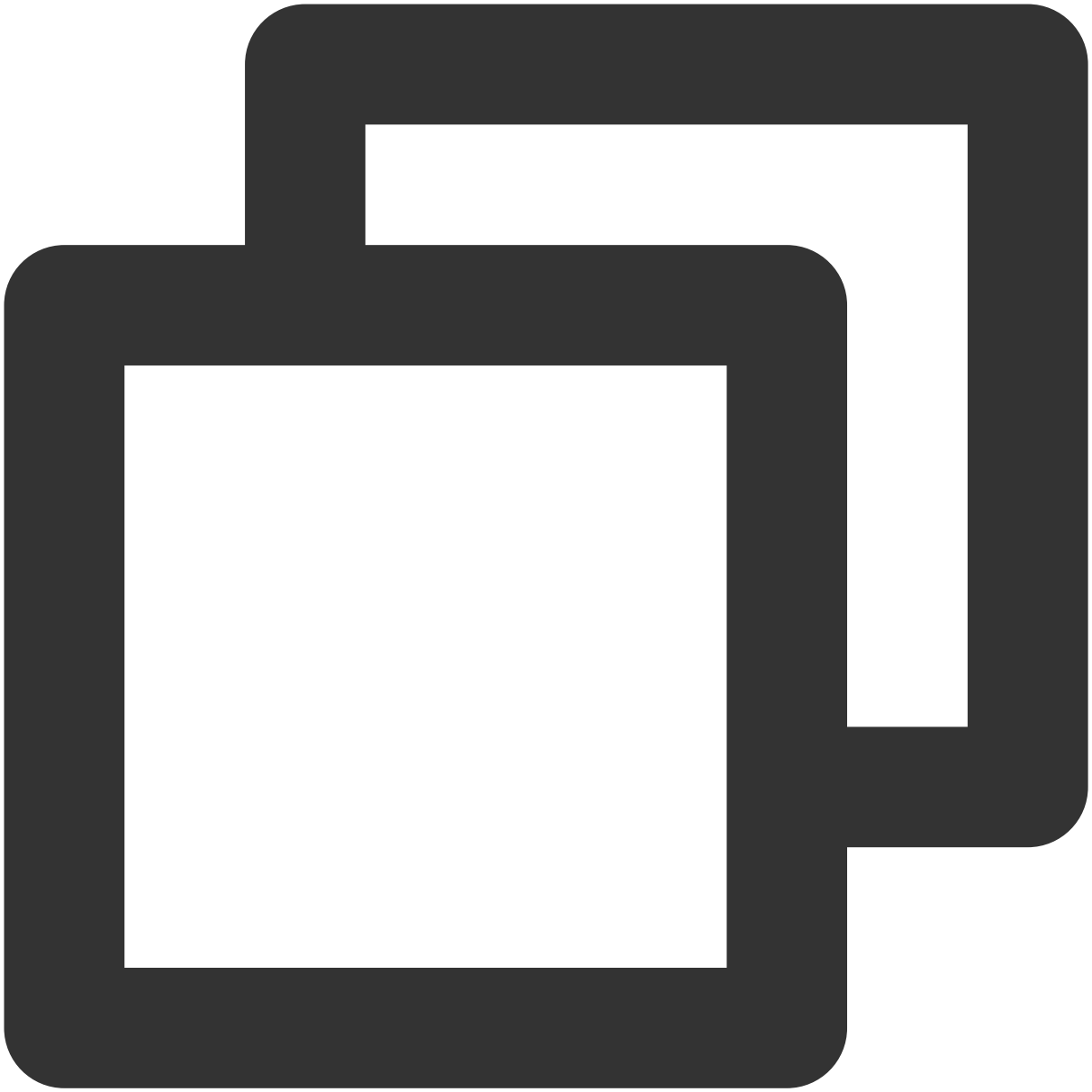
Waktu update terbaru：2023-06-15 14:59:31

## Skenario

Jika tidak dapat memasang cloudinit di citra Linux Anda, gunakan **Forced Image Import** (Impor Citra Secara Paksa) untuk mengimpor citra. Jika Anda menggunakan citra ini untuk impor, yang tidak menginstal cloudinit, Tencent Cloud tidak dapat menginisialisasi CVM Anda. Dalam hal ini, Anda perlu menyiapkan skrip sendiri untuk mengonfigurasi CVM berdasarkan file konfigurasi yang disediakan oleh Tencent Cloud. Dokumen ini menjelaskan cara mengonfigurasi CVM jika citra diimpor secara paksa.
Tencent Cloud memberi pengguna perangkat CDROM yang berisi informasi konfigurasi. Pengguna perlu memasang CDROM dan membaca informasi `mount_point/qcloud_action/os.conf` untuk konfigurasi. Jika data konfigurasi lain atau UserData perlu digunakan, pengguna dapat langsung membaca file di bawah `mount_point/` .

## File Konfigurasi os.conf

Konten os.conf adalah sebagai berikut.



```
hostname=VM_10_20_xxxx
password=GRSgae1fw9frsG.rfrF
eth0_ip_addr=10.104.62.201
eth0_mac_addr=52:54:00:E1:96:EB
eth0_netmask=255.255.192.0
eth0_gateway=10.104.0.1
dns_nameserver="10.138.224.65 10.182.20.26 10.182.24.12"
```

**Keterangan:**

Nama parameter di atas adalah untuk referensi, dan nilainya hanya digunakan sebagai contoh.

Deskripsi masing-masing parameter dalam file konfigurasi os.conf adalah sebagai berikut:

| Nama Parameter | Deskripsi |
| --- | --- |
| nama host | Nama CVM |
| kata sandi | Kata sandi terenkripsi |
| eth0_ip_addr | IP LAN dari eth0 |
| eth0_mac_addr | Alamat MAC dari eth0 |
| eth0_netmask | Subnet mask dari eth0 |
| eth0_gateway | Gateway eth0 |
| dns_nameserver | Server resolusi DNS |

## Batas

Citra harus memenuhi batas pada citra Linux sebagaimana diuraikan dalam Impor Citra, kecuali untuk cloudinit.
Partisi sistem untuk mengimpor citra tidak lengkap.
Citra yang diimpor tidak berisi kerentanan yang dapat dieksploitasi dari jarak jauh.
Sebaiknya ubah kata sandi segera setelah instans berhasil dibuat dengan citra yang diimpor secara paksa.

## Catatan

Perhatikan hal berikut saat mengonfigurasi penguraian skrip:
Skrip dijalankan secara otomatis saat startup. Harap terapkan persyaratan ini berdasarkan sistem operasi Anda.
Pasang `/dev/cdrom` dan baca file `qcloud_action/os.conf` di bawah titik pemasangan untuk mendapatkan informasi konfigurasi.
Kata sandi yang ditempatkan di CDROM oleh Tencent Cloud sudah dienkripsi. Anda dapat mengatur kata sandi baru dengan `chpasswd -e` .
**Note that the encrypted password may contain special characters. We recommend you place it in a file and then set the password with `chpasswd -e < passwd_file` . (Perhatikan bahwa kata sandi terenkripsi mungkin berisi karakter khusus. Sebaiknya Anda menempatkannya dalam file, lalu atur kata sandi dengan `chpasswd -e < passwd_file` .)**
Saat Anda menggunakan citra yang diimpor secara paksa untuk membuat instans dan kemudian membuat citra, Anda perlu memastikan bahwa skrip akan tetap dijalankan untuk memastikan bahwa instans dikonfigurasi dengan benar. Anda juga dapat menginstal cloudinit dalam instans ini.

# Petunjuk

**Perhatian:**

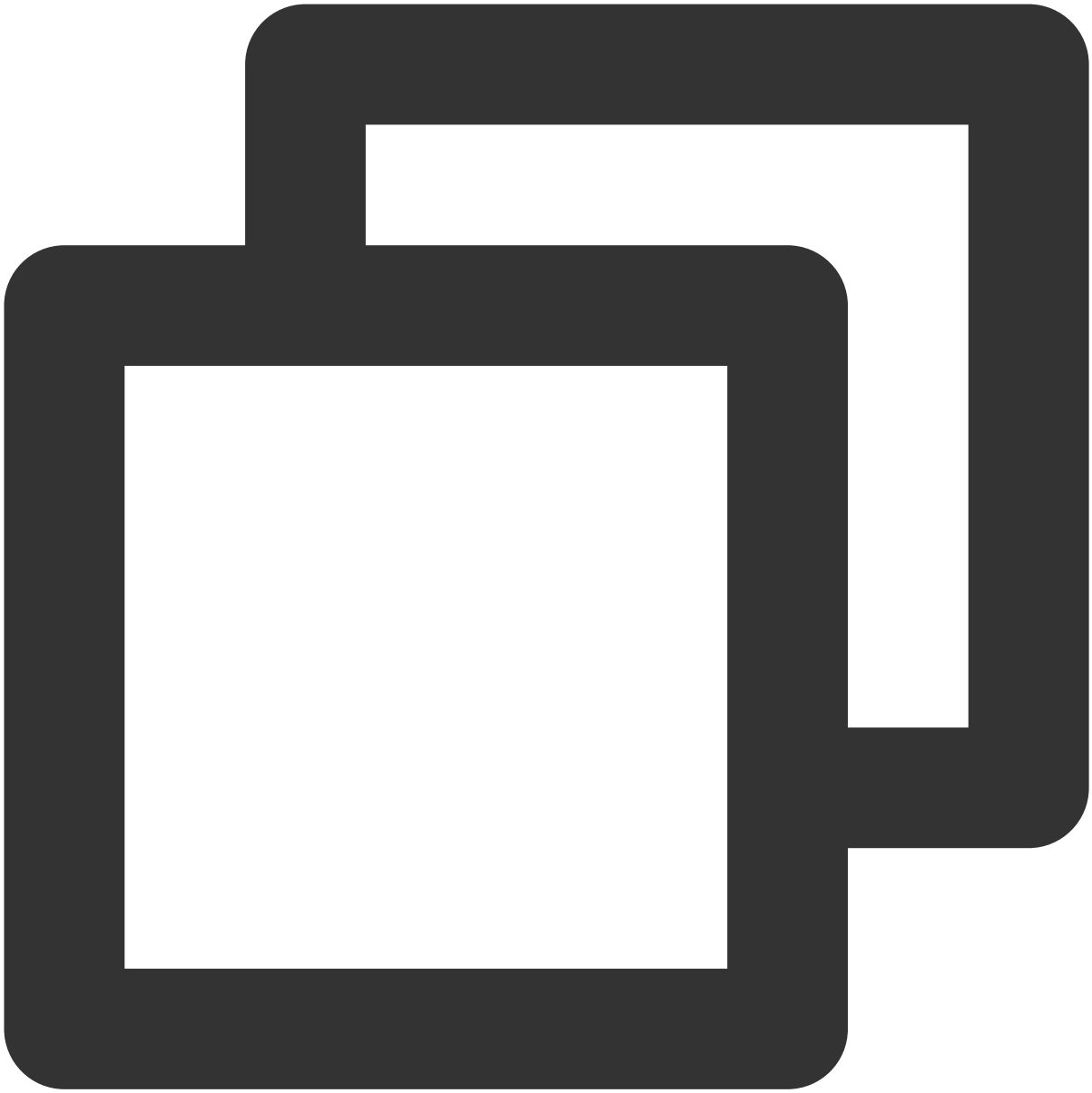
Tencent Cloud menyediakan contoh skrip berdasarkan CentOS. Anda dapat menjadikannya rujukan guna membuat skrip untuk citra Anda. Selama pembuatan, perhatikan bahwa:

**The script must be properly placed in the system before image import** (Skrip harus ditempatkan dengan benar di sistem sebelum impor citra).

Skrip ini tidak berlaku untuk semua sistem operasi. Anda perlu memodifikasinya sesuai dengan sistem operasi Anda sendiri.

1. Buat skrip `os_config` berdasarkan contoh skrip berikut.

Anda dapat memodifikasi skrip sesuai kebutuhan.

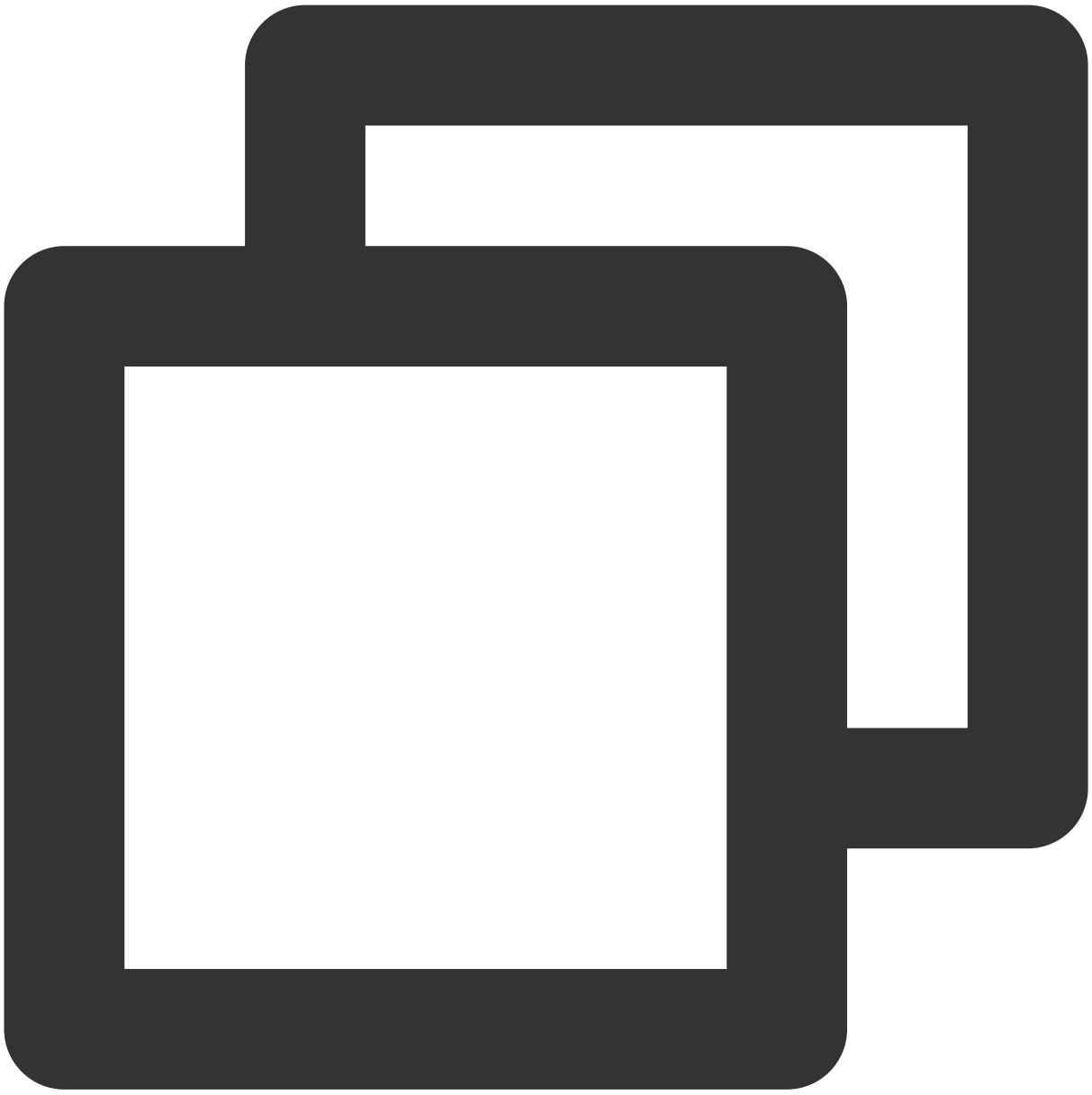


```
#!/bin/bash
### BEGIN INIT INFO
# Provides:          os-config
# Required-Start:    $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: config of os-init job
# Description: run the config phase without cloud-init
### END INIT INFO
```

```
####################user settings#####################
cdrom_path=`blkid -L config-2`
load_os_config() {
    mount_path=$(mktemp -d /mnt/tmp.XXXX)
    mount /dev/cdrom $mount_path
    if [[ -f $mount_path/qcloud_action/os.conf ]]; then
        . $mount_path/qcloud_action/os.conf
        if [[ -n $password ]]; then
            passwd_file=$(mktemp /mnt/pass.XXXX)
            passwd_line=$(grep password $mount_path/qcloud_action/os.conf)
            echo root:${passwd_line#*=} > $passwd_file
        fi
        return 0
    else
        return 1
    fi
}
cleanup() {
    umount /dev/cdrom
    if [[ -f $passwd_file ]]; then
        echo $passwd_file
        rm -f $passwd_file
    fi
    if [[ -d $mount_path ]]; then
        echo $mount_path
        rm -rf $mount_path
    fi
}
config_password() {
    if [[ -f $passwd_file ]]; then
        chpasswd -e < $passwd_file
    fi
}
config_hostname(){
    if [[ -n $hostname ]]; then
        sed -i "/^HOSTNAME=.*/d" /etc/sysconfig/network
        echo "HOSTNAME=$hostname" >> /etc/sysconfig/network
    fi
}
config_dns() {
    if [[ -n $dns_nameserver ]]; then
        dns_conf=/etc/resolv.conf
        sed -i '/^nameserver.*/d' $dns_conf
        for i in $dns_nameserver; do
            echo "nameserver $i" >> $dns_conf
        done
    fi
```

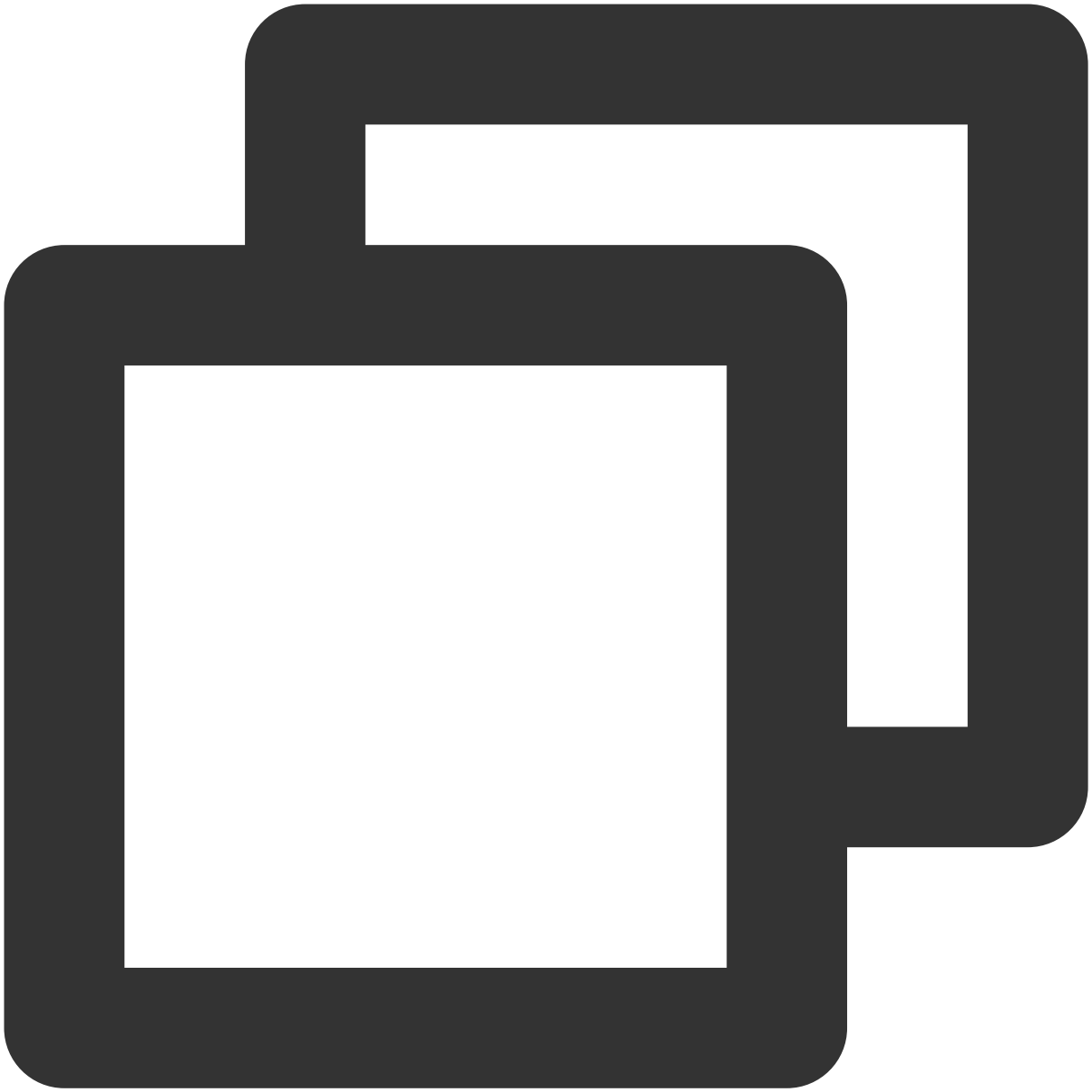
```
}
config_network() {
    /etc/init.d/network stop
    cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=$eth0_ip_addr
NETMASK=$eth0_netmask
HWADDR=$eth0_mac_addr
ONBOOT=yes
GATEWAY=$eth0_gateway
BOOTPROTO=static
EOF
    if [[ -n $hostname ]]; then
        sed -i "/^${eth0_ip_addr}.*/d" /etc/hosts
        echo "${eth0_ip_addr} $hostname" >> /etc/hosts
    fi
    /etc/init.d/network start
}
config_gateway() {
    sed -i "s/^GATEWAY=.*/GATEWAY=$eth0_gateway" /etc/sysconfig/network
}
####################init#####################
start() {
    if load_os_config ; then
        config_password
        config_hostname
        config_dns
        config_network
        cleanup
        exit 0
    else
        echo "mount ${cdrom_path} failed"
        exit 1
    fi
}
RETVAL=0
case "$1" in
    start)
        start
        RETVAL=$?
    ;;
    *)
        echo "Usage: $0 {start}"
        RETVAL=3
    ;;
esac
exit $RETVAL
```

2. Tempatkan skrip `os_config` di direktori `/etc/init.d/` dan jalankan perintah berikut.



```
chmod +x /etc/init.d/os_config
chkconfig --add os_config
```

3. Jalankan perintah berikut untuk memeriksa apakah `os_config` telah ditambahkan ke layanan startup.



```
chkconfig --list
```

**Keterangan:**

Anda harus memastikan bahwa skrip dijalankan dengan benar. Jika Anda gagal terhubung ke instans melalui SSH atau terjadi pengecualian jaringan setelah impor citra, coba hubungkan ke instans melalui konsol untuk menjalankan skrip lagi. Jika masalah tersebut masih terjadi, hubungi layanan pelanggan.

# Migrasi Layanan
# Migrasi Online
# Ikhtisar

Waktu update terbaru：2021-12-13 18:24:44

Melalui migrasi online, Anda dapat memigrasikan sistem dan aplikasi pada server sumber dari IDC Anda atau platform cloud lainnya ke Tencent Cloud. Ini memenuhi persyaratan bisnis untuk cloudifikasi perusahaan, migrasi lintas vendor, migrasi lintas akun atau lintas wilayah, dan deploymnet cloud hibrida.

**Keterangan:**

Server sumber dapat berupa server fisik, mesin virtual, atau server cloud pada platform cloud lain, seperti AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, atau Huawei Cloud.

## Kasus Penggunaan

Migrasi online berlaku untuk skenario berikut:

Cloudifikasi arsitektur TI

Deployment arsitektur cloud hibrida

Migrasi lintas-cloud

Migrasi lintas akun atau lintas wilayah

## Perbedaan dari Migrasi Offline

Dalam migrasi offline, Anda perlu membuat citra untuk disk sistem atau disk data di server sumber, lalu memigrasikan citra ke Cloud Virtual Machine (CVM) atau Cloud Block Storage (CBS). Anda tidak perlu membuat citra untuk migrasi online. Sebagai gantinya, Anda dapat menjalankan alat migrasi di server sumber untuk memigrasikannya ke CVM tujuan.

## Fitur

Saat ini, migrasi online mendukung fitur migrasi server.

## Persiapan

Daftarkan akun Tencent Cloud dan siapkan CVM tujuan.
Hentikan aplikasi di server sumber untuk mencegah aplikasi yang ada agar tidak terpengaruh oleh migrasi.
Klik di sini untuk mengunduh paket alat migrasi terkompresi.
Periksa apakah server sumber dan CVM tujuan memenuhi persyaratan migrasi. Misalnya, disk cloud CVM tujuan harus memiliki kapasitas yang cukup untuk menyimpan data yang dimigrasikan dari server sumber.

## Memulai Migrasi

Gunakan go2tencentcloud yang disediakan oleh Tencent Cloud untuk migrasi. Untuk informasi selengkapnya tentang alat tersebut, lihat Alat Migrasi Online.

## Pertanyaan Umum

Untuk informasi selengkapnya, harap lihat Tentang Migrasi Layanan.

# Migrasi Offline

Waktu update terbaru：2021-12-13 18:24:45

## Ikhtisar

Migrasi Layanan adalah platform yang dikembangkan oleh Tencent Cloud untuk membantu perusahaan memigrasikan sistem operasi, aplikasi, dan data aplikasi dari server sumber ke Cloud Virtual Machine (CVM) atau Cloud Block Storage (CBS). Migrasi ini membantu memenuhi kebutuhan perusahaan akan cloudifikasi, migrasi lintas cloud, migrasi lintas akun atau lintas wilayah, dan deployment cloud hibrida.
Migrasi layanan mencakup migrasi offline dan migrasi online. Migrasi offline meliputi:
Migrasi instans offline memungkinkan Anda memigrasi citra disk sistem ke CVM tertentu.
Migrasi data offline memungkinkan Anda memigrasikan citra disk data ke CBS tertentu.

## Prasyarat

Migrasi offline memerlukan Cloud Object Storage (COS). Pastikan wilayah Anda didukung oleh COS.
Untuk informasi selengkapnya tentang wilayah yang didukung oleh COS, lihat Wilayah dan Titik Akhir Akses.

## Persiapan

**Perhatian:**
Saat ini, migrasi layanan Tencent Cloud mendukung citra dalam format qcow2, vhd, vmdk, dan mentah. Sebaiknya gunakan format citra terkompresi untuk mempersingkat waktu transmisi dan migrasi.
Wilayah COS tempat citra diunggah harus sama dengan tempat CVM yang ingin Anda migrasikan berada.
Selama migrasi offline, ukuran file citra yang diunggah tidak boleh lebih besar dari kapasitas disk yang ingin Anda migrasikan. Jika ukuran file citra adalah 50 GB, disk sistem harus setidaknya 50 GB.
Migrasi offline tidak mendukung snapshot (nama file mirip dengan *-00000*.vmdk).
Buat citra untuk server yang perlu dimigrasikan seperti yang diinstruksikan dalam dokumentasi pembuatan citra.
Untuk Windows, lihat Menyiapkan Citra Windows.
Untuk Linux, lihat Menyiapkan Citra Linux.
Unggah file citra yang dibuat ke COS.
Karena file citra berukuran besar, unggah menggunakan browser mungkin gagal. Sebaiknya gunakan alat COSCMD untuk mengunggah citra. Untuk informasi selengkapnya, lihat COSCMD.

Jika citra yang diekspor dari platform cloud lain adalah paket terkompresi (seperti file .tar.gz), Anda dapat mengunggahnya langsung ke COS.
Dapatkan alamat COS dari citra yang diunggah.
Di konsol COS, cari file citra yang baru saja Anda unggah dan lihat informasinya untuk mendapatkan tautan file.
Siapkan CVM atau CBS yang akan dimigrasikan.
Klik di sini untuk membeli CVM >>.
Klik di sini untuk melihat petunjuk pembelian CBS >>.

# Petunjuk

### Migrasi instans offline

1. Login ke konsol CVM, lalu klik **Service Migration** ([Migrasi Layanan]) di bilah sisi kiri.
2. Klik **Create an instans migration task** (Buat tugas migrasi instans).
3. Selesaikan langkah-langkah persiapan seperti yang diminta, dan klik **Next** (Selanjutnya).
4. Pilih wilayah, masukkan informasi konfigurasi seperti nama tugas, tautan COS, dan instans CVM yang akan dimigrasikan. Kemudian, klik **Complete** (Selesai) untuk membuat tugas migrasi.

Selama migrasi, Anda dapat keluar atau menutup halaman Migrasi Layanan. Anda juga dapat kembali ke halaman ini kapan saja untuk memeriksa kemajuan tugas.

**Perhatian:**

File COS harus dikonfigurasi dengan izin baca/tulis pribadi. Untuk informasi selengkapnya, lihat Mengatur Izin Akses Objek.
Kapasitas disk sistem dari instans yang ingin Anda migrasikan tidak boleh kurang dari ukuran file citra yang diunggah. Jika tidak, tugas akan gagal.

### Migrasi data offline

1. Login ke konsol CVM, lalu klik **Service Migration** ([Migrasi Layanan]) di bilah sisi kiri.
2. Klik **Create a data migration task** (Buat tugas migrasi data).
3. Selesaikan langkah-langkah persiapan seperti yang diminta, dan klik **Next** (Selanjutnya).
4. Pilih wilayah, masukkan informasi konfigurasi seperti nama tugas, tautan COS, dan disk cloud yang akan dimigrasikan. Kemudian, klik **Complete** (Selesai) untuk membuat tugas migrasi.

Selama migrasi, Anda dapat keluar atau menutup halaman Migrasi Layanan. Anda juga dapat kembali ke halaman ini kapan saja untuk memeriksa kemajuan tugas.

**Perhatian:**

Kapasitas disk CBS yang ingin Anda migrasikan tidak boleh kurang dari ukuran file citra yang diunggah. Jika tidak, tugas akan gagal.

# Pertanyaan Umum

Untuk informasi selengkapnya, lihat Tentang Migrasi Layanan.

# Hubungi Kami

Waktu update terbaru：2021-12-13 18:24:46

Jika Anda mengalami masalah selama migrasi layanan, atau memiliki umpan balik atau saran, jangan ragu untuk menghubungi kami.

## Mengirimkan Tiket

Jika Anda mengalami masalah operasi atau teknis saat menggunakan produk kami, Anda dapat login ke Tencent Cloud Console dan mengikuti petunjuk di layar untuk mengirimkan tiket. Kami akan segera menghubungi Anda.
Tautan tiket:
Mengirimkan tiket: Kirim tiket
Mengkueri status tiket: Daftar tiket

# Cloud Block Storage
# Memperluas Disk Cloud

Waktu update terbaru：2021-12-13 18:24:47

## Ikhtisar

Disk cloud adalah perangkat penyimpanan yang dapat diperluas di cloud. Setelah disk cloud dibuat, Anda dapat memperluas kapasitasnya kapan saja untuk meningkatkan kapasitas penyimpanannya tanpa kehilangan data apa pun di dalamnya.
Setelah disk cloud diperluas, Anda perlu menetapkan kapasitas yang diperluas ke partisi yang ada, atau memformatnya menjadi partisi baru yang independen. Untuk informasi selengkapnya, lihat Memperluas Partisi dan Sistem File (Windows) atau Memperluas Partisi dan Sistem File (Linux).

**Perhatian:**

Partisi MBR mendukung disk dengan kapasitas maksimum 2 TB. Saat Anda mempartisi disk dengan kapasitas lebih besar dari 2 TB, kami sarankan Anda membuat dan memasang disk data baru dan menggunakan format partisi GPT untuk menyalin data.

## Memperluas Disk Data

Jika disk cloud adalah disk data, Anda dapat memperluasnya menggunakan tiga metode berikut.

**Perhatian:**

Jika beberapa disk cloud dengan kapasitas dan jenis yang sama dipasang ke CVM, Anda dapat membedakannya menurut metode yang ditunjukkan dalam Membedakan disk data. Pilih disk data dan perluas kapasitasnya dengan cara berikut.

**Memperluas disk data melalui konsol CVM (direkomendasikan)**

1. Login ke konsol CVM.
2. Temukan CVM tempat Anda ingin memperluas disk data, dan pilih **More** (Lainnya) > **Resource Adjustment** (Penyesuaian Sumber Daya) > **Expand Data Disk** (Perluas Disk Data) di kolom **Operation** (Operasi).
3. Pilih disk data yang akan diperluas di jendela pop-up, dan klik **Next** (Selanjutnya).
4. Pilih kapasitas baru (harus lebih besar atau sama dengan kapasitas saat ini.) dan klik **Next** (Selanjutnya).
5. Baca catatan dan klik **Adjust Now** (Sesuaikan Sekarang).
6. Tetapkan kapasitasnya yang diperluas ke partisi yang ada, atau format menjadi partisi baru yang independen. Tergantung pada sistem operasi CVM, lihat Memperluas Partisi dan Sistem File (Windows) atau Memperluas Partisi dan Sistem File (Linux).

#### Memperluas disk data melalui konsol CBS

1. Login ke konsol CBS.
2. Cari disk cloud yang akan diperluas, dan pilih **More** (Lainnya) > **Expand** (Perluas) di kolom **Operation** (Operasi).
3. Pilih kapasitas baru. Kapasitas harus lebih besar dari atau sama dengan kapasitas saat ini.
4. Selesaikan pembayaran.
5. Tetapkan kapasitasnya yang diperluas ke partisi yang ada, atau format menjadi partisi baru yang independen. Tergantung pada sistem operasi CVM, lihat Memperluas Partisi dan Sistem File (Windows) atau Memperluas Partisi dan Sistem File (Linux).

#### Memperluas disk data melalui API

Anda dapat menggunakan `ResizeDisk` API untuk memperluas disk cloud yang ditentukan. Untuk informasi selengkapnya, lihat ResizeDisk.

## Memperluas Disk Sistem

Jika disk cloud berfungsi sebagai disk sistem, Anda dapat memperluasnya menggunakan dua metode berikut.

#### Memperluas disk sistem melalui konsol CVM (direkomendasikan)

1. Login ke konsol CVM. Temukan CVM tempat Anda ingin memperluas disk sistem, lalu pilih **More** (Lainnya) > **Resource Adjustment** (Penyesuaian Sumber Daya) > **Expand System Disk** (Perluas Disk Sistem) di kolom **Operation** (Operasi).
2. Pilih disk sistem yang akan diperluas di jendela pop-up, lalu klik **Next** (Selanjutnya).
3. Pilih kapasitas baru (harus lebih besar atau sama dengan kapasitas saat ini.) dan klik **Next** (Selanjutnya).
4. Baca catatannya, pilih **Agree to a force shutdown** (Setujui pematian paksa), lalu klik **Adjust Now** (Sesuaikan Sekarang).
5. Setelah perluasan selesai di konsol, periksa konfigurasi cloudinit untuk instans Linux atau instans Windows sesuai dengan sistem operasi CVM. Kemudian, perluas partisi dan sistem file sesuai kebutuhan.

#### Memperluas disk sistem dengan menginstal ulang sistem

Anda juga dapat memperluas disk sistem dengan menginstal ulang sistem

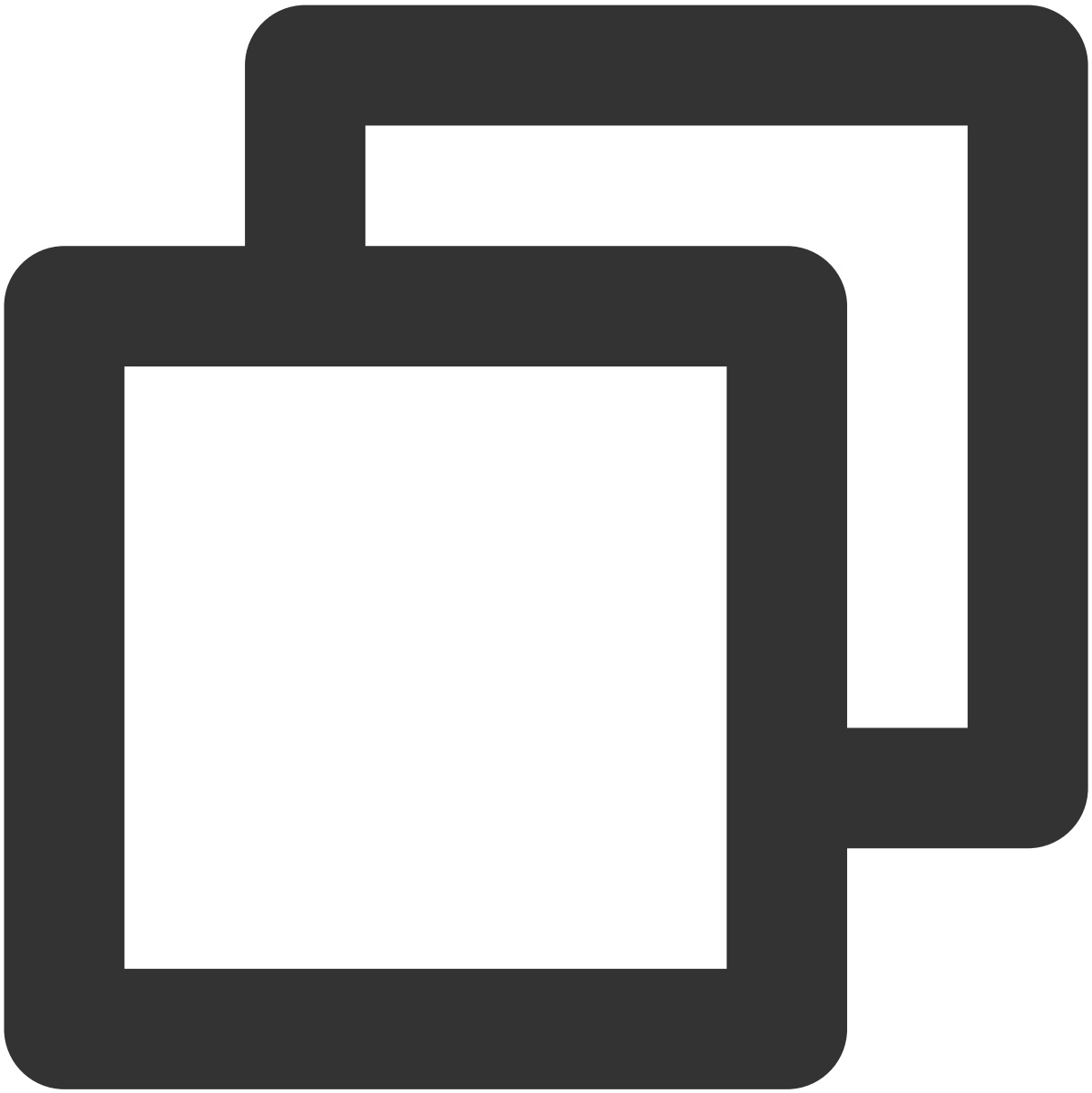
## Operasi

### Membedakan disk data

Periksa disk cloud sesuai dengan sistem operasi CVM.

#### Linux

1. Login ke instans Linux
2. Jalankan perintah berikut untuk melihat hubungan antara disk cloud elastis dan nama perangkat.



```
ls -l /dev/disk/by-id
```

Informasi berikut akan muncul:

```
[root@VM_63_126_centos ~]# ls -l /dev/disk/by-id/
total 0
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-35t32l8g -> ../../vdf
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-je13nl0g -> ../../vdc
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-jwz43lpg -> ../../vde
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-punhzcju -> ../../vdd
```

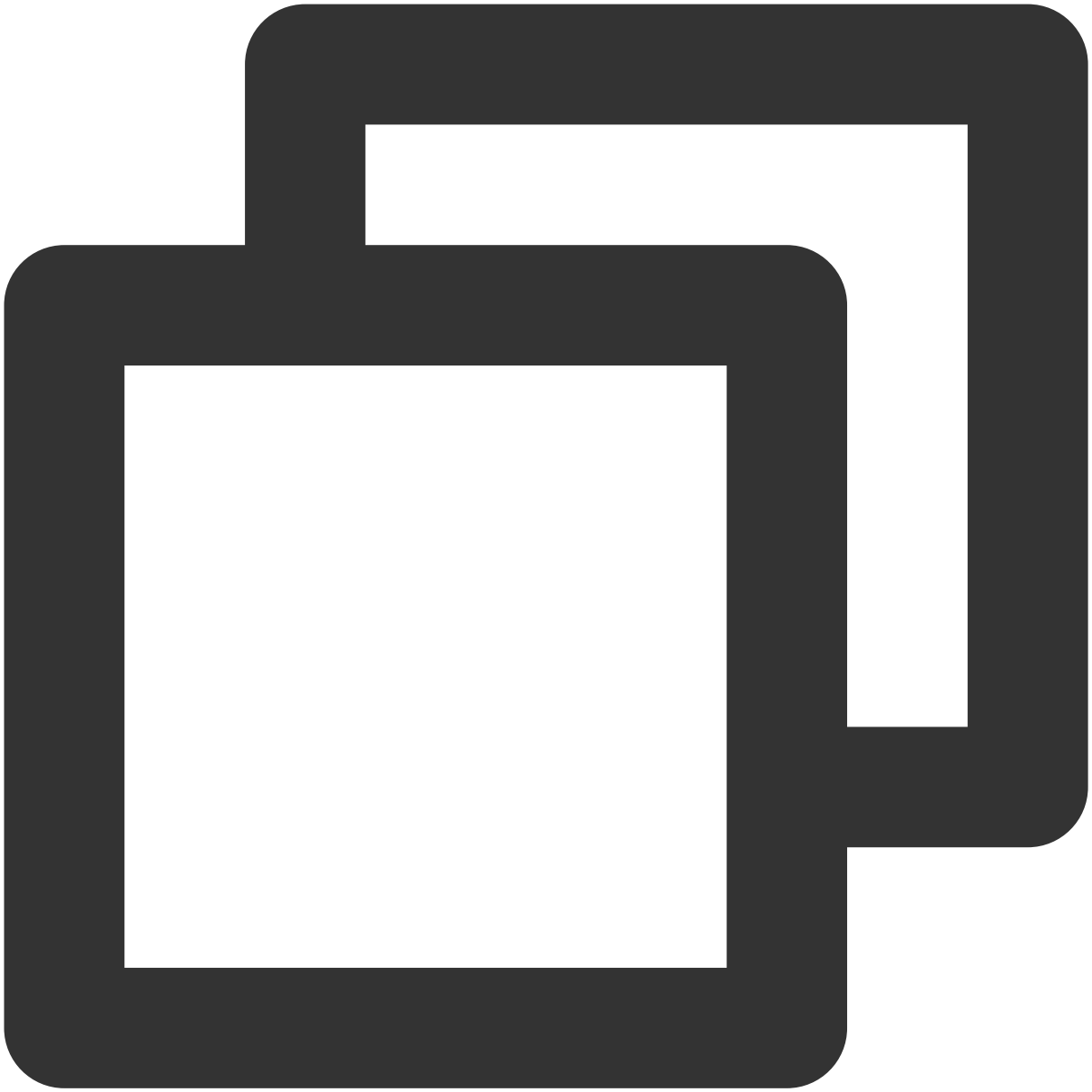
Perhatikan bahwa `disk-xxxx` adalah ID dari disk cloud. Anda dapat menggunakannya untuk melihat detail disk cloud di konsol CBS.

### Windows

1. Login ke instans Windows.
2. Klik kanan

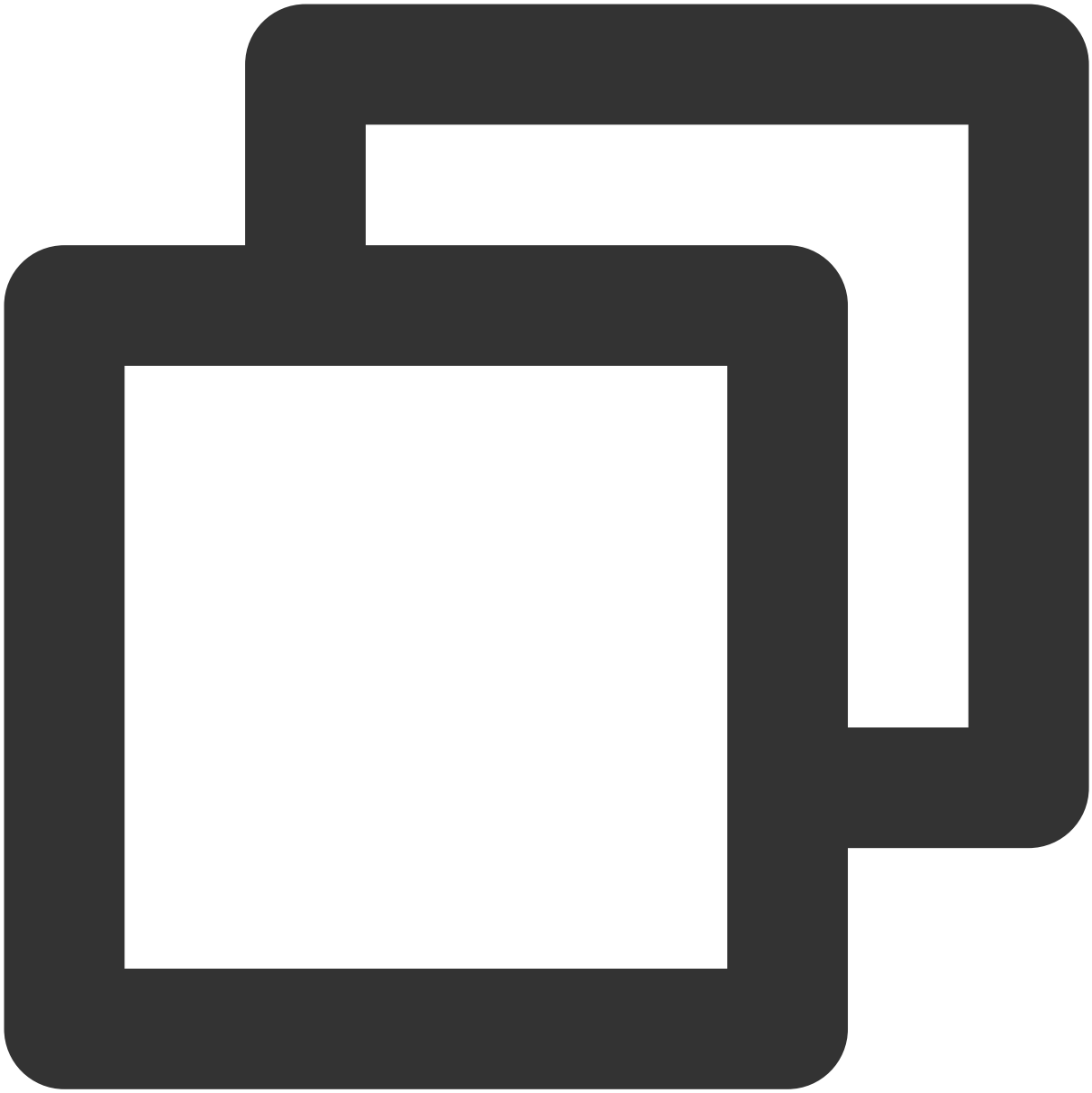
, lalu pilih **Run** (Jalankan).

3. Masukkan `cmd` di jendela pop-up, lalu tekan **Enter** (Enter).
4. Jalankan perintah berikut untuk melihat hubungan antara disk cloud elastis dan nama perangkat.



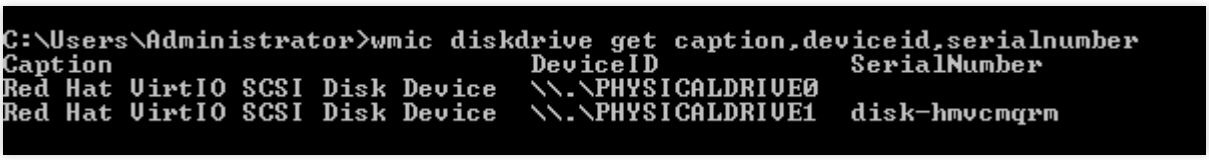
```
wmic diskdrive get caption,deviceid,serialnumber
```

Anda juga dapat menjalankan perintah berikut



```
wmic path win32_physicalmedia get SerialNumber,Tag
```

Informasi berikut akan muncul:




Perhatikan bahwa `disk-xxxx` adalah ID dari disk cloud. Anda dapat menggunakannya untuk melihat detail disk

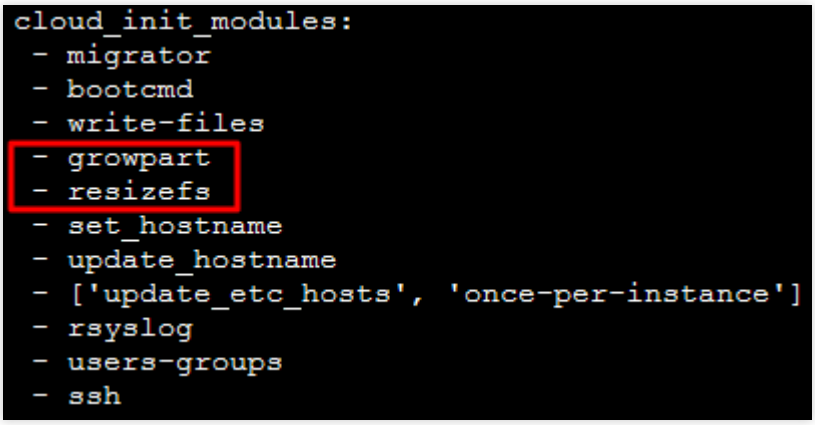
cloud di konsol CBS.

## Memeriksa konfigurasi cloudinit

Periksa konfigurasi cloudinit sesuai dengan sistem operasi CVM.

### Memeriksa konfigurasi cloudinit untuk instans Linux

Setelah disk sistem diperluas, login ke instans Linux dan periksa apakah file `/etc/cloud/cloud.cfg` berisi item konfigurasi `growpart` dan `resizefs`.
Jika ya, abaikan operasi lainnya.




**growpart** (growpart): memperluas partisi ke ukuran disk.
**resizefs** (resizefs): memperluas atau menyesuaikan sistem file partisi `/` ke ukuran partisi.
Jika tidak, secara manual memperluas partisi dan sistem file (Linux) sesuai dengan sistem operasi, dan menetapkan kapasitas yang diperluas ke partisi yang ada, atau memformatnya menjadi partisi baru yang independen.

### Memeriksa konfigurasi cloudinit untuk instans Windows

Setelah disk sistem diperluas, login ke instans Windows dan periksa apakah item konfigurasi `ExtendVolumesPlugin` ada di bawah `plugin` di `C:\\Program Files\\Cloudbase Solutions\\Cloudbase-Init\\conf \\cloudbase-init.conf`.
Jika ya, abaikan operasi lainnya.
Jika tidak, secara manual perluas partisi dan sistem file (Windows) sesuai dengan sistem operasi, dan tetapkan kapasitas yang diperluas ke partisi yang ada, atau ubah formatnya menjadi partisi baru yang independen.

# Mengubah Jenis Media Disk

Waktu update terbaru：2021-12-13 18:24:47

## Ikhtisar

Tencent Cloud CVM mendukung penyesuaian media perangkat keras penyimpanan, yang memungkinkan Anda merespons secara fleksibel kebutuhan penyimpanan yang beragam dari berbagai bisnis.
Tencent Cloud menyediakan dua jenis media penyimpanan: Cloud Block Storage dan [Local Storage atau Penyimpanan Lokal](https://www.tencentcloud.com/document/product/ 213/5798). Disk lokal dapat dikonversi ke disk cloud. Dokumen ini menjelaskan cara mengubah jenis media disk.
Kelemahan CVM dengan disk lokal adalah sebagai berikut:
Konfigurasi tidak dapat disesuaikan karena keterbatasan sumber daya host.
Fitur seperti snapshot dan akselerasi pembuatan tidak didukung.
Keandalan data rendah.
Kegagalan host akan berdampak lebih lama.
Untuk menghindari kerugian ini, Anda dapat mengonversi disk lokal yang terpasang ke CVM Anda ke disk cloud.

## Prasyarat

**CVM Status** (Status CVM)
Pastikan CVM terkait dinonaktifkan.
**Unsupported CVM Types** (Jenis CVM yang Tidak Didukung)
Instans spot
Big data dan model I/O tinggi
Instans bare metal
**CVM Configuration** (Konfigurasi CVM)
Setidaknya salah satu disk sistem dan disk data CVM harus **HDD** (HDD) atau **SSD local disk** (disk lokal SSD).
Tersedia disk cloud yang ukurannya sesuai dengan disk lokal di zona ketersediaan tempat CVM berada.
Penyesuaian akan mengonversi **all** (semua) disk lokal ke disk cloud jika disk sistem dan disk data CVM adalah disk lokal. Anda juga dapat mengonfigurasi jenis disk cloud untuk setiap disk secara terpisah.
Dengan kata lain, perubahan media disk dari CVM yang disk-nya adalah semua disk lokal berlaku untuk semua disk-nya, bukan hanya disk sistem atau disk data.
Mengubah media cloud disk tidak akan mengubah ukuran disk. Anda dapat memperluas disk cloud setelah mengubah jenis media.

Operasi ini tidak akan mengubah siklus pemakaian CVM, ID instans, IP pribadi/publik, nama disk, dan titik pemasangan.

## Catatan

Konversi ini perlu menyalin semua data dari disk lokal ke disk cloud. Tergantung pada ukuran disk dan kecepatan transmisi, proses ini bisa memakan waktu.
Anda hanya dapat mengonversi disk lokal ke disk cloud. Konversi TIDAK DAPAT dikembalikan.
**After the adjustment, we recommend you to start up and log in to the CVM to check the data integrity** (Setelah penyesuaian, sebaiknya mulai dan login ke CVM untuk memeriksa integritas data).

## Petunjuk

1. Login ke Konsol CVM dan akses halaman **Instances* (Instans).
**Keterangan:**
Jika CVM telah dinonaktifkan, lanjutkan ke Langkah 3.
2. (Opsional) Cari CVM target, lalu klik **More** (Lainnya) > **Instance Status** (Status Instans) > **Shutdown** (Nonaktifkan) di bawah kolom **Operation** (Operasi) untuk menonaktifkannya.
3.
Di bawah kolom **Operation**
(Operasi), klik **More** (Lainnya) > **Resource Adjustment** (Penyesuaian Sumber Daya) > **Change Disk Media Type** (Ubah Jenis Media Disk).
4. Di jendela pop-up, pilih jenis disk cloud target, centang **I have read and agreed to Rules for Changing Disk Media Type** (Saya telah membaca dan menyetujui Aturan untuk Mengubah Jenis Media Disk), lalu klik **Change Now** (Ubah Sekarang).
5. Periksa kembali informasinya, lakukan pembayaran jika berlaku, dan tunggu hingga prosesnya selesai.

# Menyesuaikan Jenis Disk Cloud

Waktu update terbaru：2021-12-13 18:24:47

Performa disk cloud tergantung pada kapasitasnya. Anda dapat meningkatkan performanya dengan menyesuaikan kapasitasnya hingga mencapai batas. Saat batas tercapai, Anda dapat membeli performa ekstra untuk mendapatkan performa yang lebih tinggi. Perhatikan bahwa performa ekstra hanya tersedia untuk instans SSD yang ditingkatkan. Untuk informasi selengkapnya, lihat Performa SSD yang Ditingkatkan.

**Perhatian:**

Saat ini, hanya **Enhanced SSD** (SSD yang Ditingkatkan) yang mendukung penyesuaian performa independen. Performa ekstra dapat disesuaikan secara independen hanya setelah performa dasar mencapai batas maksimal. Penyesuaian performa tidak akan memengaruhi pengoperasian disk cloud dan bisnis Anda.

## Penagihan Penyesuaian Performa

### Peningkatan

Untuk disk cloud bayar sesuai pemakaian, peningkatan performa akan segera berlaku, dan disk cloud langsung diisi oleh konfigurasi baru.

### Penurunan

Untuk disk cloud bayar sesuai pemakaian, peningkatan performa akan segera berlaku, dan disk cloud langsung diisi oleh konfigurasi baru.

## Peningkatan Performa

#### Meningkatkan disk melalui konsol

Ketika prasyarat terpenuhi, Anda dapat meningkatkan disk seperti yang diinstruksikan di bawah ini di konsol:

1. Login ke konsol CBS.
2. Pilih wilayah dan disk cloud yang memerlukan penyesuaian performa.
3. Klik **More** (Lainnya) > **Adjust Performance** (Sesuaikan Performa) di bawah kolom **Operation** (Operasi) dari disk cloud yang dipilih.
4. Pilih konfigurasi target di jendela pop-up.
5. Baca dan konfirmasi catatan, lalu mulai penyesuaian.

#### Meningkatkan disk melalui API

Anda juga dapat menggunakan `ModifyDiskExtraPerformance` API untuk meningkatkan disk cloud tertentu. Untuk petunjuk mendetail, lihat ModifyDiskExtraPerformance.

# Penurunan Performa

### Menurunkan disk melalui konsol

Ketika prasyarat terpenuhi, Anda dapat menurunkan versi disk seperti yang diinstruksikan di bawah ini di konsol:

1. Login ke konsol CBS.
2. Pilih wilayah dan disk cloud yang memerlukan penyesuaian performa.
3. Klik **More** (Lainnya) > **Adjust Performance** (Sesuaikan Performa) di bawah kolom **Operation** (Operasi) dari disk cloud yang dipilih.
4. Pilih konfigurasi target di jendela pop-up.
5. Baca dan konfirmasi catatan, lalu mulai penyesuaian.

### Menurunkan disk melalui API

Anda juga dapat menggunakan `ModifyDiskExtraPerformance` API untuk menurunkan disk cloud tertentu. Untuk petunjuk mendetail, lihat ModifyDiskExtraPerformance.

# Jaringan
# Beralih ke VPC

Waktu update terbaru：2024-01-02 10:28:57

## Ikhtisar

Tencent Cloud menyediakan jaringan klasik dan VPC untuk berbagai skenario. Berbagai fitur ditawarkan untuk membantu Anda mengelola jaringan secara fleksibel.
Beralih antar jaringan:
**Switching from the classic network to VPC** (Beralih dari jaringan klasik ke VPC): Tencent Cloud memungkinkan Anda memigrasikan satu atau beberapa instans CVM dari jaringan klasik ke VPC sekaligus.
**Switching between VPCs** (Beralih antara VPC): Tencent Cloud memungkinkan Anda memigrasikan satu atau beberapa instans CVM dari VPC A ke VPC B sekaligus.
Menentukan alamat IP kustom.
Memilih untuk mempertahankan HostName.

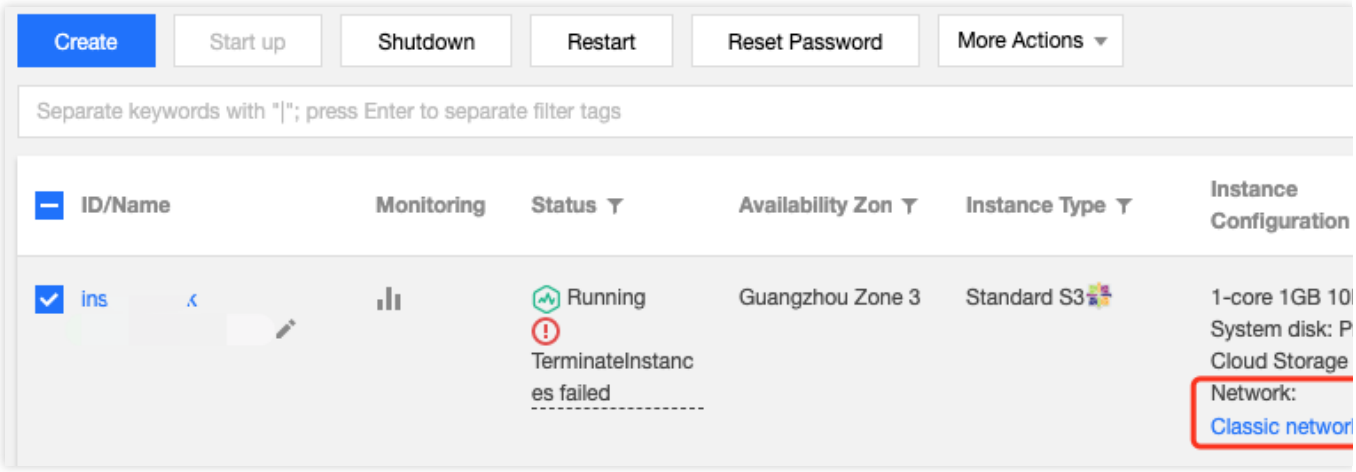
## Prasyarat

Sebelum migrasi, lepas ikatan instans CVM dari CLB dan ENI di jaringan pribadi dan publik dan lepaskan alamat IP sekunder dari ENI primer. Ikat ulang instans setelah migrasi.

## Petunjuk

### Menentukan atribut jaringan dari instans CVM

1. Login ke konsol CVM.
2. Di halaman **Instances** (Instans), temukan instans target yang ingin Anda migrasikan.
Instans ada di jaringan klasik jika “Jaringan: Jaringan Klasik” muncul di kolom **Instance Configuration** (Konfigurasi Instans), seperti yang ditunjukkan di bawah ini:




**Perhatian:**

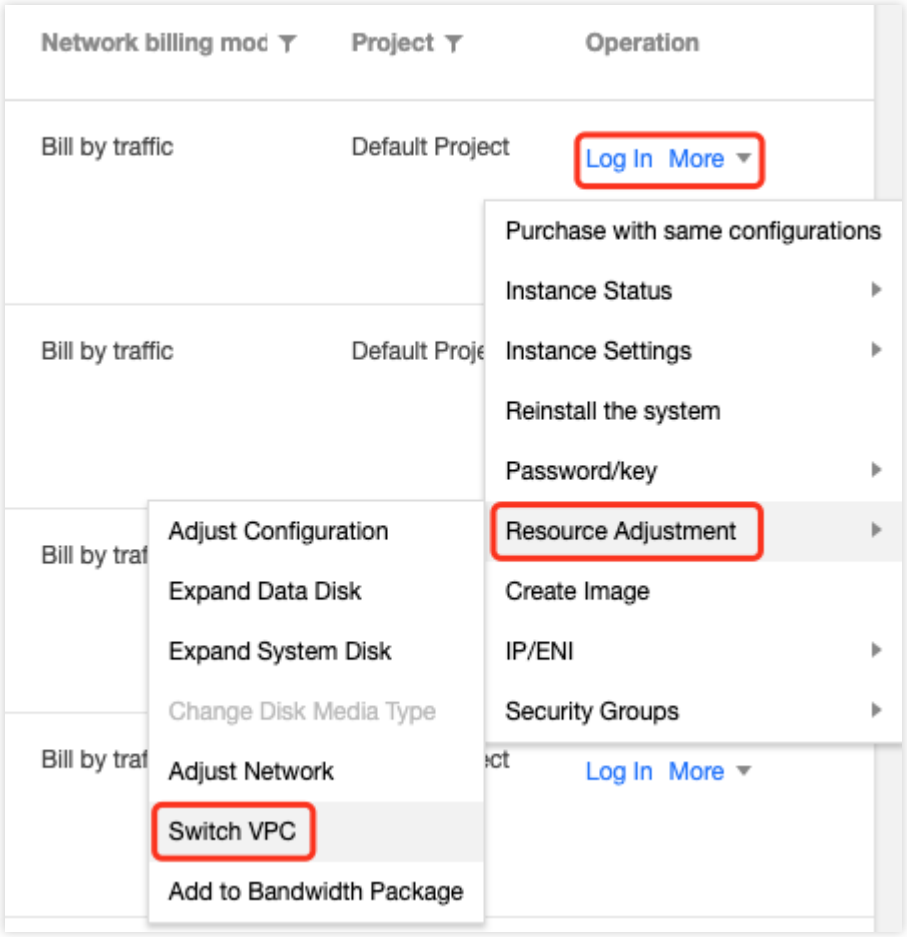
Migrasi dari jaringan klasik ke VPC TIDAK DAPAT dikembalikan. Setelah migrasi, instans CVM tidak akan dapat berkomunikasi dengan layanan Tencent Cloud di jaringan klasik.

Setelah Anda menentukan atribut jaringan instans CVM, Anda dapat memigrasikan instans ke VPC sesuai kebutuhan.

## Memigrasikan ke VPC

1. Login ke konsol CVM.
2. Di halaman **Instances** (Instans), migrasikan instans target ke VPC.

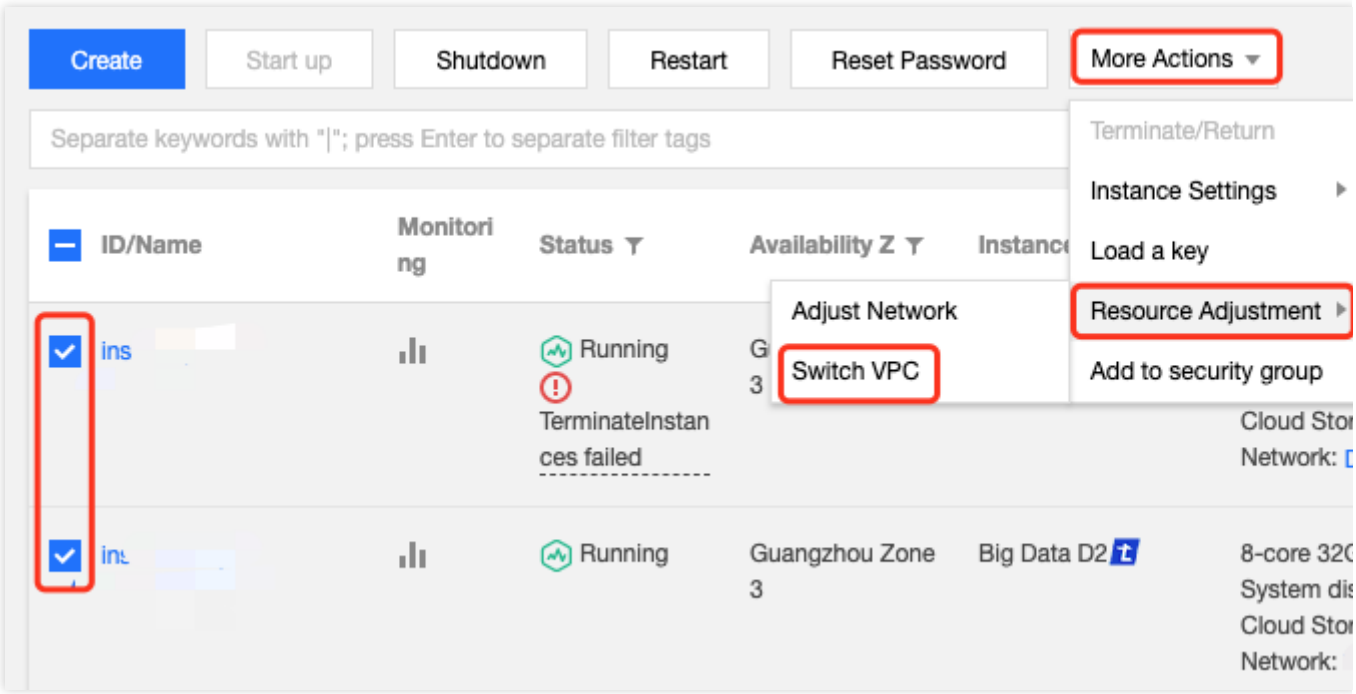
**Method 1** (Metode 1): untuk memigrasikan instans ke VPC, cari dan pilih **More** (Lainnya) -> **Resource Adjustment** (Penyesuaian Sumber Daya) -> **Switch VPC** (Beralih VPC) di kolom **Operation** (Operasi).




**Method 2** (Metode 2): untuk mengelompokkan instans ke VPC, pilih instans target, lalu klik **More Actions** (Tindakan Lainnya) -> **Resource Adjustment** (Penyesuaian Sumber Daya) -> **Switch VPC** (Beralih VPC) di bagian atas daftar instans.

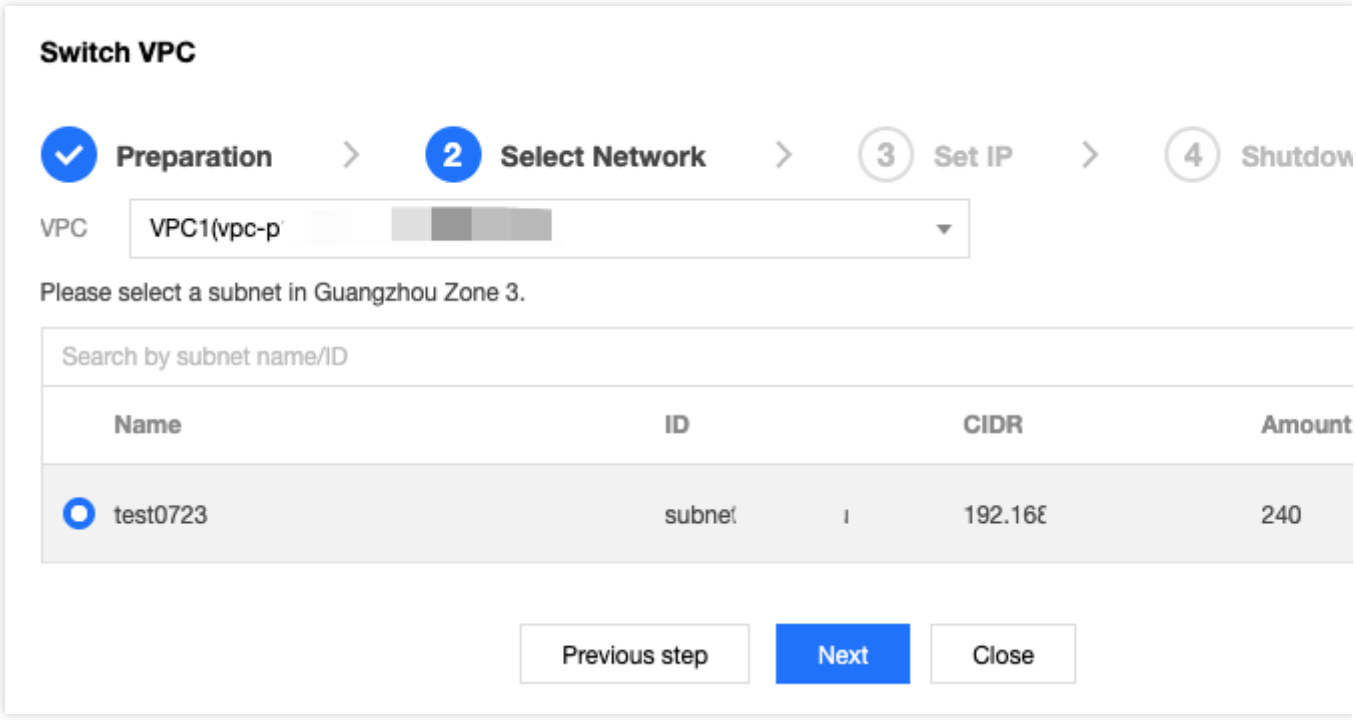
**Perhatian:**

Migrasi massal hanya didukung untuk instans CVM di zona ketersediaan yang sama.




3. Di jendela **Switch VPC** (Beralih VPC) yang muncul, baca catatannya, lalu klik **Next** (Selanjutnya).

4. Pilih VPC tujuan dan subnet yang sesuai, lalu klik **Next** (Selanjutnya).

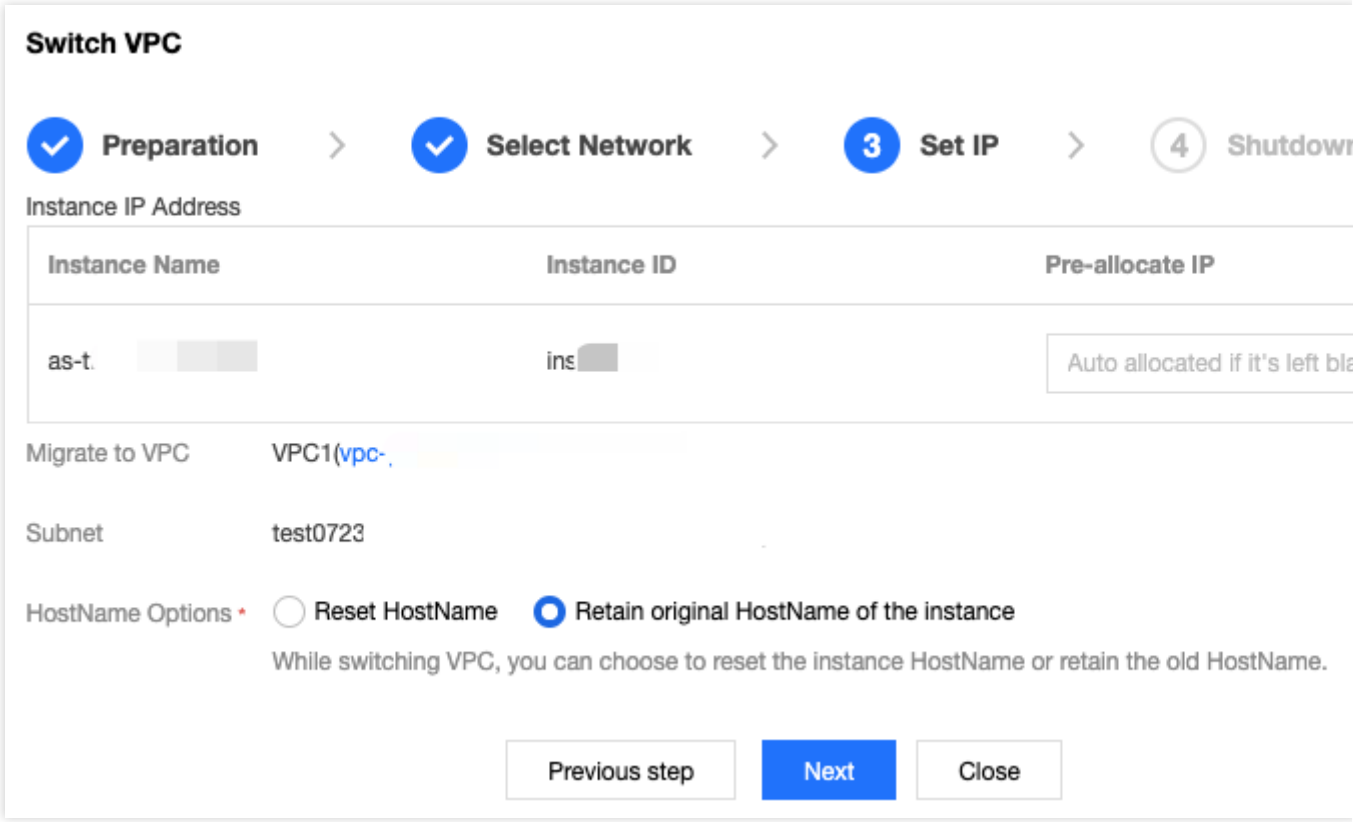



5. Tentukan alamat IP yang telah ditetapkan sebelumnya dan opsi HostName untuk **Set IP** (Menetapkan IP) sesuai kebutuhan, lalu klik **Next** (Selanjutnya).

**Keterangan:**

Jika tidak ada alamat IP yang ditentukan sebelumnya, sistem akan secara otomatis menetapkan alamat IP.

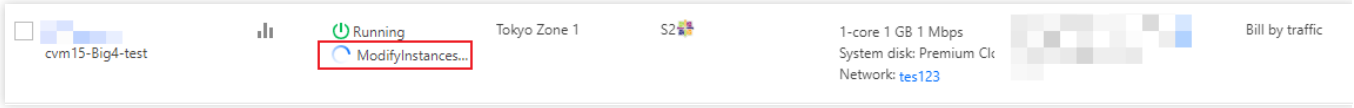
Saat menentukan opsi HostName, Anda dapat memilih **Reset HostName** (Atur ulang HostName) atau **Retain the original HostName of the instance** (Pertahankan HostName instans asli).




6. Lakukan operasi sesuai petunjuk di halaman **Shutdown CVM** (Mematikan CVM), lalu klik **Start Migration** (Mulai Migrasi). Setelah migrasi selesai, Anda dapat login ke konsol CVM. Pada halaman **Instances** (Instans), Anda akan melihat bahwa **Modifying instance VPC attributes** (Memodifikasi atribut VPC instans) ditampilkan di kolom **Status** (Status) dari instans yang dimigrasikan.

**Perhatian:**

Selama migrasi, instans CVM perlu dimulai ulang. Dengan demikian, jangan melakukan operasi lain selama waktu ini. Periksa status instans setelah migrasi dan verifikasi apakah akses jaringan pribadi dan login jarak jauh berfungsi dengan baik.



# IP Elastis

Waktu update terbaru：2022-09-23 16:16:06

## Skenario

Elastic IP, atau EIP, adalah IP statis yang dirancang untuk komputasi cloud dinamis dan IP publik tetap di wilayah tertentu. Dengan EIP, Anda dapat memetakan ulang dengan cepat alamat ke instans lain di akun Anda atau instans gateway NAT untuk menghindari kegagalan instans. Dokumen ini menjelaskan cara menggunakan EIP.

## Prasyarat

Anda telah login ke Konsol CVM.

## Petunjuk

### Mengajukan EIP

1. Di bilah sisi kiri, klik **EIP** ([EIP]) untuk masuk ke halaman pengelolaan EIP.
2. Klik **Apply** (Ajukan) di halaman pengelolaan EIP.
3. Di jendela pop-up “Apply for EIP” (Ajukan EIP), pilih wilayah, jenis alamat IP, metode penagihan, dan batas bandwidth, lalu masukkan jumlah EIP yang ingin Anda ajukan.
4. Klik **OK** (OKE) untuk menyelesaikan aplikasi EIP.
5. Setelah aplikasi selesai, Anda dapat melihat di daftar EIP yang Anda ajukan, yang dalam status tidak terikat.

### Mengikat EIP ke produk cloud

1. Di bilah sisi kiri, klik **EIP** ([EIP]) untuk masuk ke halaman pengelolaan EIP.
2. Di halaman pengelolaan EIP, pilih EIP yang ingin Anda ikat ke produk cloud dan klik **More** (Lainnya) > **Bind** (Ikat).

**Perhatian:**

Jika EIP telah terikat pada instans, harap lepaskan terlebih dahulu.

3. Di jendela pop-up “Bind resources” (Ikat sumber daya), pilih sumber daya yang akan diikat ke EIP dan klik **OK** (OKE).
4. Di jendela pop-up, klik **OK** (OKE) untuk menyelesaikan pengikatan EIP ke produk cloud.

### Melepaskan EIP dari produk cloud

1. Di bilah sisi kiri, klik **EIP** ([EIP]) untuk masuk ke halaman pengelolaan EIP.

2. Di halaman pengelolaan EIP, pilih EIP yang ingin Anda lepaskan dari produk cloud dan klik **More** (Lainnya) > **Unbind** (Lepaskan).
3. Di jendela pop-up “Unbind EIP” (Lepaskan EIP), konfirmasikan informasi pelepasan dan klik **OK** (OKE).
4. Di jendela pop-up, klik **OK** (OKE) untuk menyelesaikan pelepasan EIP dari produk cloud.

**Perhatian:**

Setelah pelepasan, instans produk cloud dapat menerima IP publik baru, yang mungkin berbeda dari IP sebelum pengikatan.

## Merilis EIP

1. Di bilah sisi kiri, klik **EIP** ([EIP]) untuk masuk ke halaman pengelolaan EIP.
2. Di halaman pengelolaan EIP, pilih EIP yang ingin Anda rilis dari produk cloud dan klik **More** (Lainnya) > **Release** (Rilis).
3. Di jendela pop-up “Are you sure you want to release the selected EIPs?” (Anda yakin ingin merilis EIP yang dipilih?), pilih **Release the above EIPs** (Rilis EIP di atas) dan klik **Release** (Rilis).

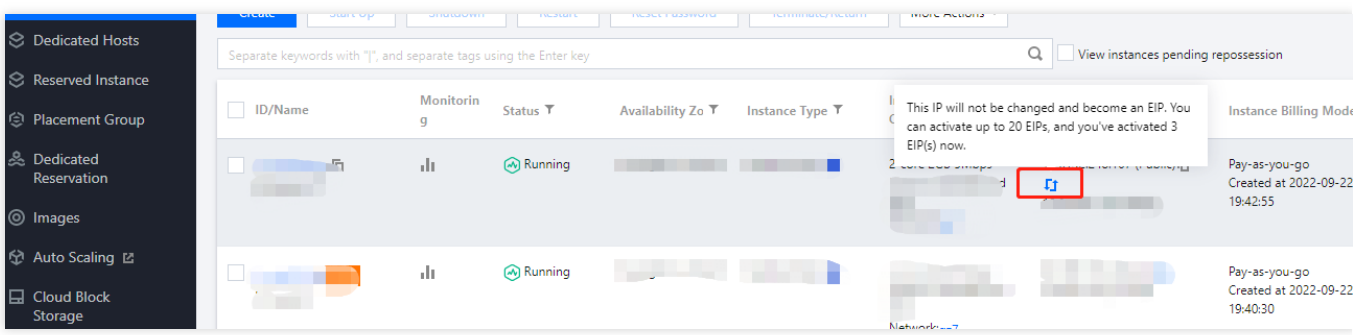
## Menyesuaikan Bandwidth

1. Di bilah sisi kiri, klik **EIP** ([EIP]) untuk masuk ke halaman pengelolaan EIP.
2. Pilih EIP yang bandwidth-nya perlu disesuaikan dan klik **Adjust Bandwidth** (Sesuaikan Bandwidth)
3. Di jendela pop-up “Adjust Bandwidth” (Sesuaikan Bandwidth), konfigurasikan nilai bandwidth dan klik **OK** (OKE) untuk menyelesaikan penyesuaian.

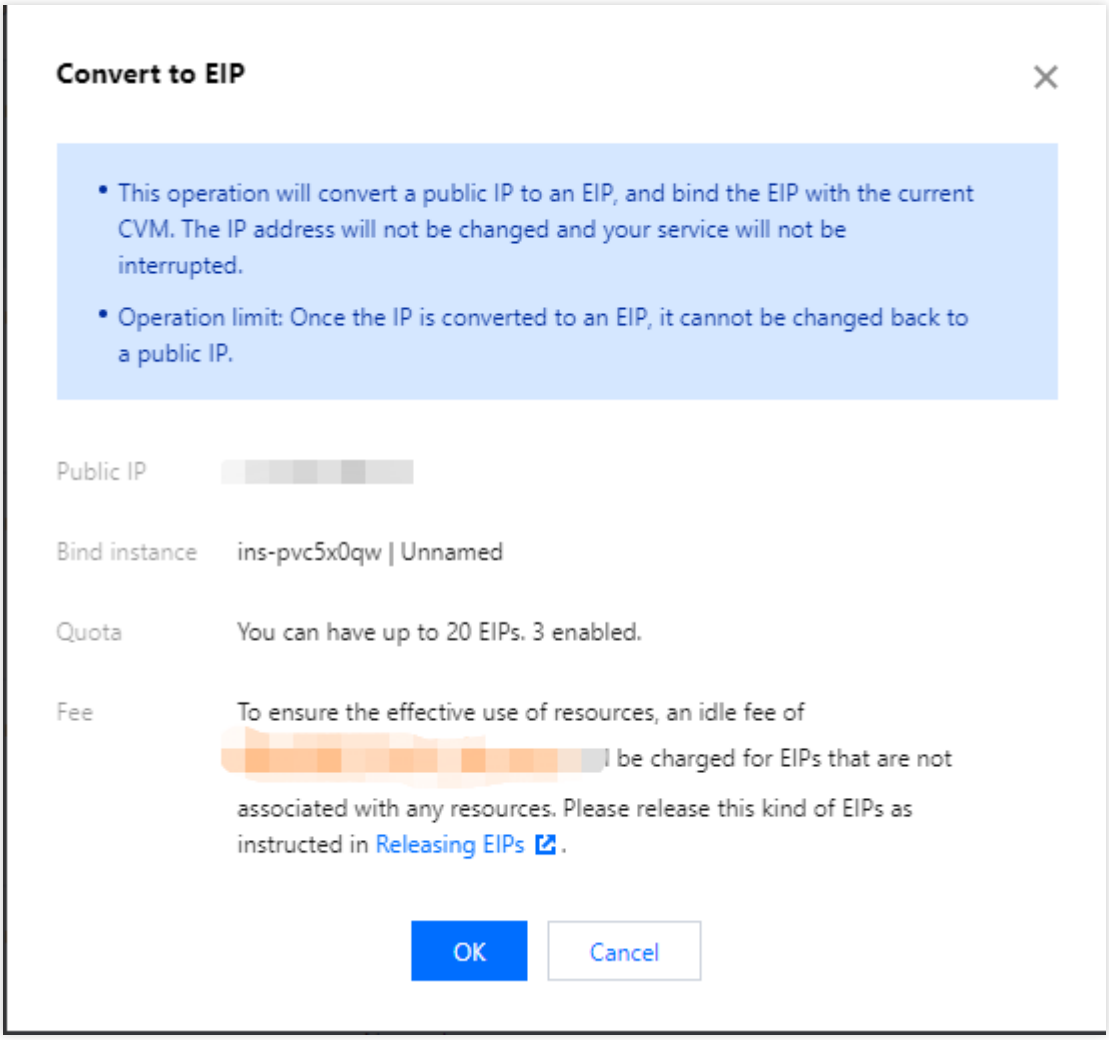
## Mengonversi IP publik menjadi EIP

IP publik yang dibeli bersama dengan instans CVM tidak elastis dan tidak dapat dipasang atau dilepas. Tencent Cloud memungkinkan Anda mengonversi IP publik ke EIP dengan langkah-langkah berikut:
1. Di bilah sisi kiri, klik **Instances** (Instans) untuk masuk ke halaman pengelolaan instans.
2. Pilih instans yang IP publiknya perlu dikonversi ke EIP, lalu klik

, seperti yang ditunjukkan di bawah ini:




3. Di jendela pop-up “Convert to EIP” (Konversikan ke EIP), klik **OK** (OKE).




# Memecahkan Masalah Pengecualian

Tidak dapat diaksesnya jaringan dapat terjadi dengan EIP karena alasan berikut:

EIP tidak terikat dengan produk cloud apa pun. Untuk informasi selengkapnya tentang cara mengikat EIP ke produk cloud, harap lihat Mengikat EIP ke produk cloud.

Kebijakan keamanan tidak valid. Periksa apakah ada kebijakan keamanan yang valid (grup keamanan atau ACL jaringan). Jika produk cloud terikat memiliki kebijakan grup keamanan, seperti akses ke port 8080 ditolak, port 8080 EIP juga tidak dapat diakses.

# ENI

Waktu update terbaru：2021-12-13 18:24:46

Untuk mengonfigurasi ENI untuk CVM Anda, ikuti petunjuk ini:

1. Buat ENI.

Lihat ENI yang baru saja Anda buat.

2. Ikat ENI ke CVM Anda, lalu konfigurasikan.

3. Konfigurasikan tabel rute CVM dan VPC.

4. Tetapkan IP pribadi.

4.1 Login ke Virtual Private Cloud Console.

4.2 Klik **ENI** (ENI) di bawah **IP and ENI** (IP dan ENI) di bilah kiri. Halaman ENI akan muncul.

4.3 Klik **ID/Name** (ID/Nama) dari ENI untuk melihat detailnya.

4.4 Klik **IP Management** (Pengelolaan IP) untuk membuka halaman detail.

4.5 Klik **Assign private IP** (Tetapkan IP pribadi) untuk menetapkan IP pribadi ke ENI. Jika Anda melakukan manual ini, pilih IP pribadi yang dapat digunakan. Klik **OK** (OKE).

5. Kelola ENI.

Merilis IP pribadi

Melepas Ikatan CVM

Menghapus ENI

Mengikat EIP

Melepas Ikatan EIP

Memodifikasi IP pribadi primer

Mengubah subnet dari ENI

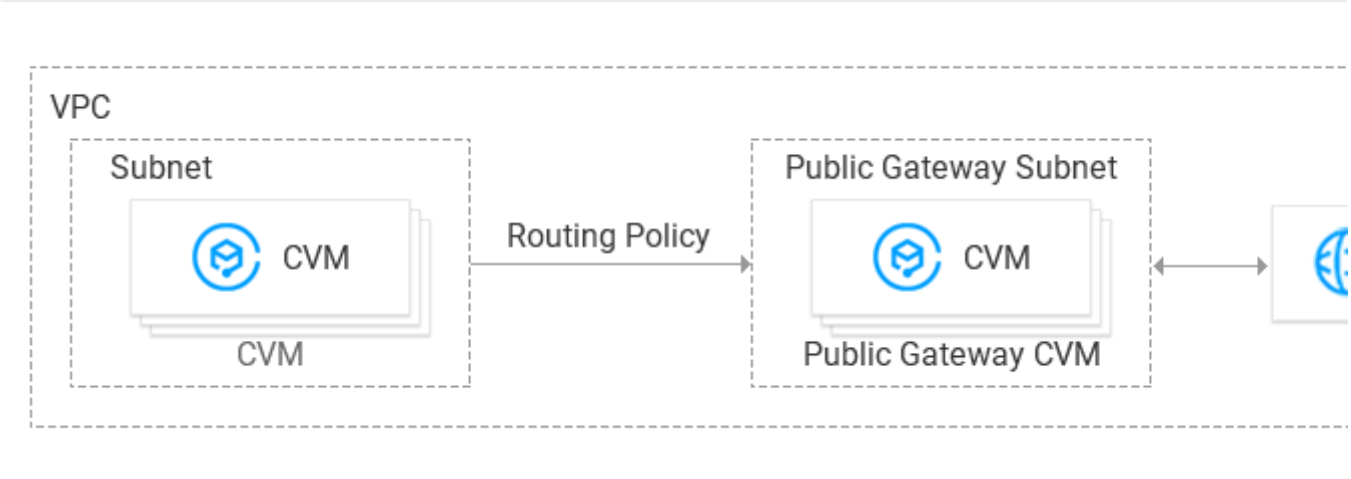
# Mengonfigurasi Gateway Publik

Waktu update terbaru：2021-12-13 18:24:46

**Keterangan:**
Mulai 6 Desember 2019, Tencent Cloud tidak lagi mendukung konfigurasi Public Network Gateway saat membeli CVM. Jika Anda perlu mengonfigurasi gateway, ikuti petunjuk ini.

## Skenario

Jika beberapa CVM Anda di Tencent Cloud VPC tidak memiliki alamat IP publik umum tetapi perlu mengakses Internet, Anda dapat menggunakan CVM dengan IP publik (IP publik umum atau elastis) sebagai gateway publik agar dapat mengakses Internet. CVM gateway publik menerjemahkan IP sumber lalu lintas keluar. Ketika CVM lain mengakses Internet melalui CVM gateway publik, CVM gateway publik menerjemahkan IP mereka ke IP publik CVM gateway publik, seperti yang ditunjukkan pada gambar di bawah.




## Prasyarat

Login ke Konsol CVM.
CVM gateway publik dan CVM yang perlu mengakses Internet melalui CVM gateway publik terletak di subnet yang berbeda karena CVM gateway publik hanya dapat meneruskan permintaan perutean dari subnet lain.
CVM gateway publik harus berupa CVM Linux. CVM Windows tidak dapat berfungsi sebagai gateway publik.

## Petunjuk

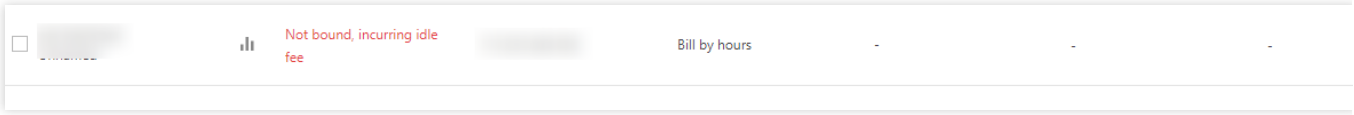
## Langkah 1: Ikat IP publik elastis (opsional)

**Keterangan:**

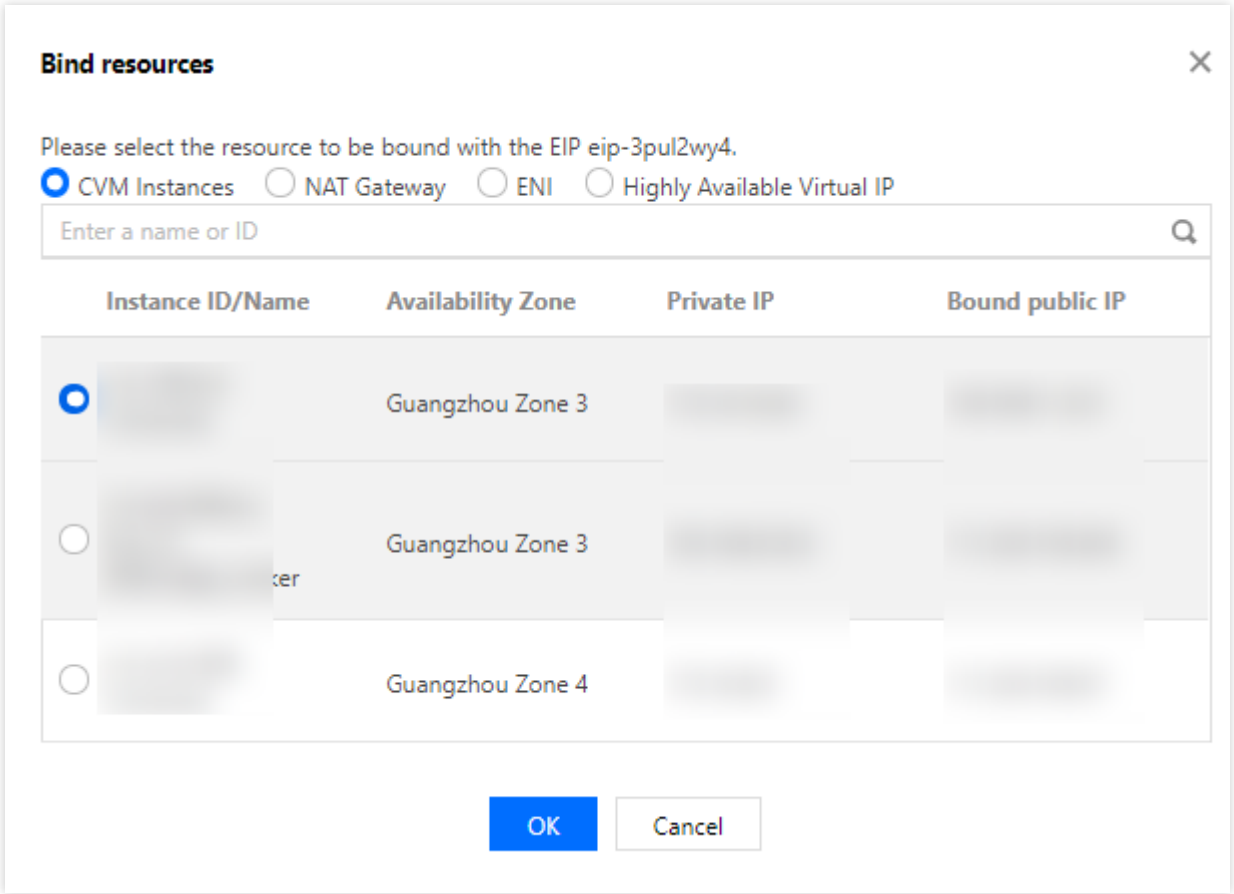
Jika CVM yang berfungsi sebagai gateway publik sudah memiliki alamat IP publik, lewati langkah ini.

1. Di panel navigasi di sebelah kiri, klik **EIP** ([EIP]) untuk membuka halaman pengelolaan EIP.

2. Temukan IP publik elastis target, lalu pilih **More** (Lainnya) > **Bind** (Ikat) di kolom **Operation** (Operasi) untuk membuka jendela **Bind resources** (Ikat sumber daya).




3. Pilih instans CVM untuk dijadikan sebagai gateway publik dan ikat ke IP publik elastis.

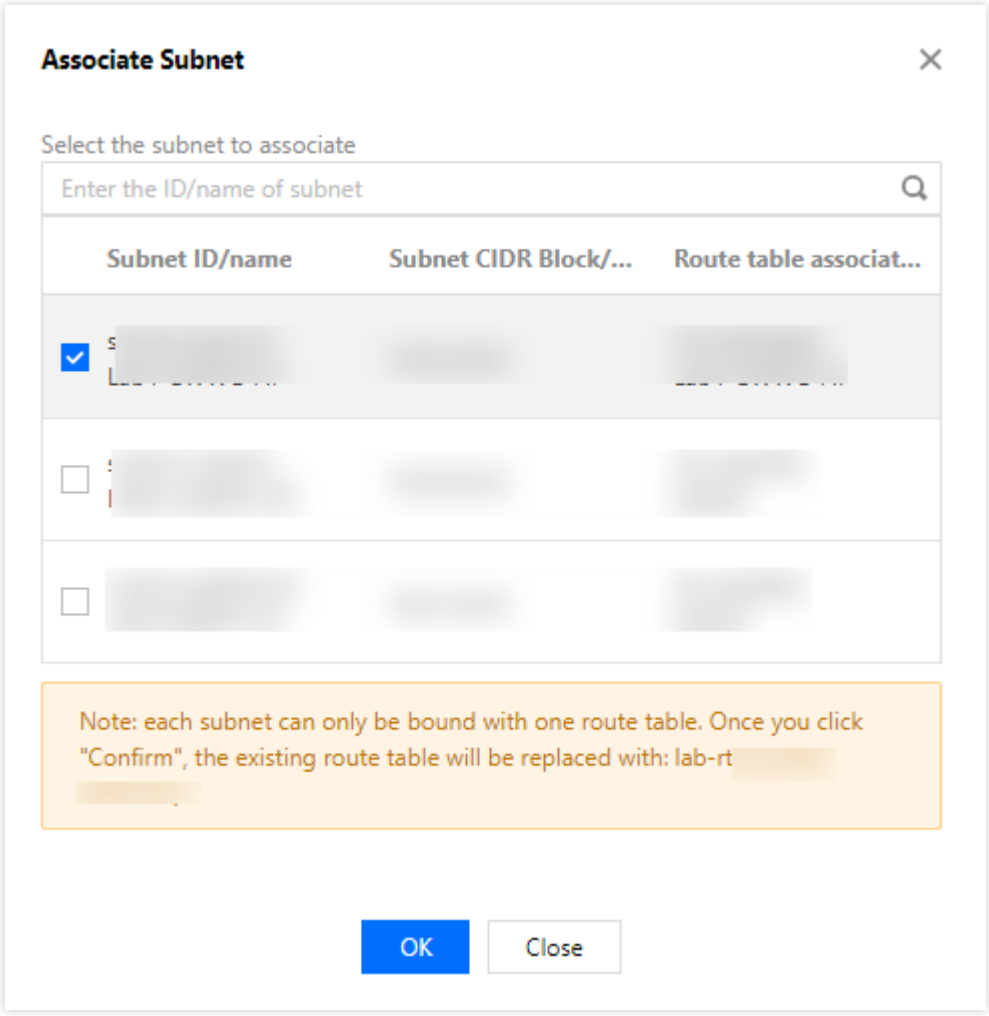



## Langkah 2: Konfigurasikan tabel perutean untuk subnet gateway

Subnet gateway dan subnet lainnya tidak dapat menggunakan tabel rute yang sama. Tabel rute terpisah harus dibuat untuk subnet gateway.

1. Buat tabel rute kustom

2. Kaitkan tabel rute dengan subnet tempat CVM gateway publik berada seperti yang diminta.




### Langkah 3: Konfigurasikan tabel rute untuk subnet lainnya

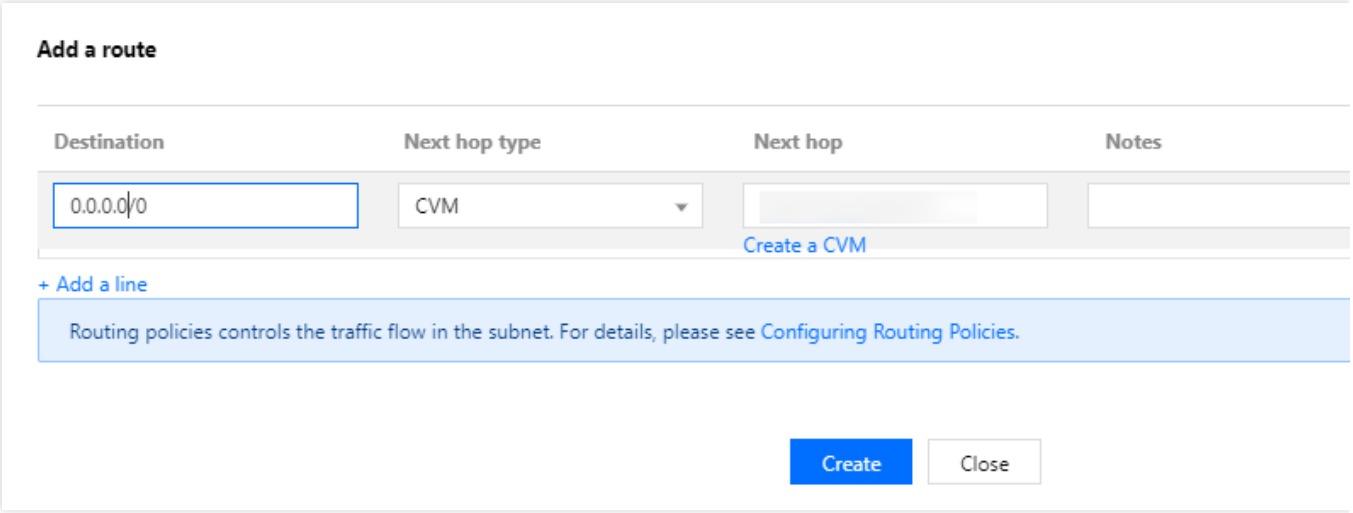
Tabel rute ini mengarahkan semua lalu lintas dari CVM tanpa IP publik ke gateway sehingga lalu lintas juga dapat mengakses jaringan publik.

Di tabel rute untuk subnet umum, tambahkan kebijakan perutean berikut:

Tujuan: IP publik yang akan diakses.

Jenis hop selanjutnya: CVM.

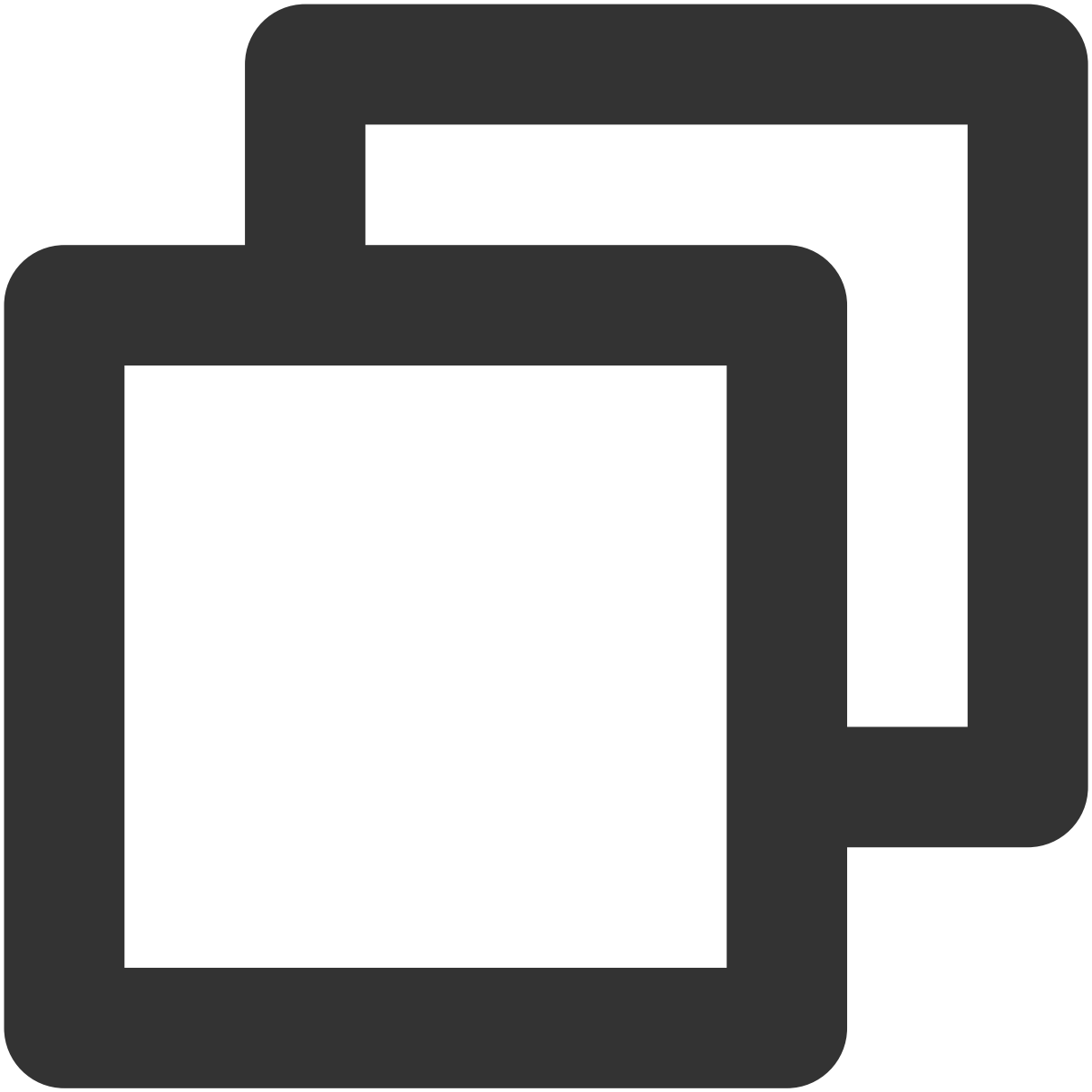
Hop selanjutnya: IP pribadi dari instans CVM tempat IP publik elastis terikat pada Langkah 1.




## Langkah 4: Konfigurasikan gateway publik

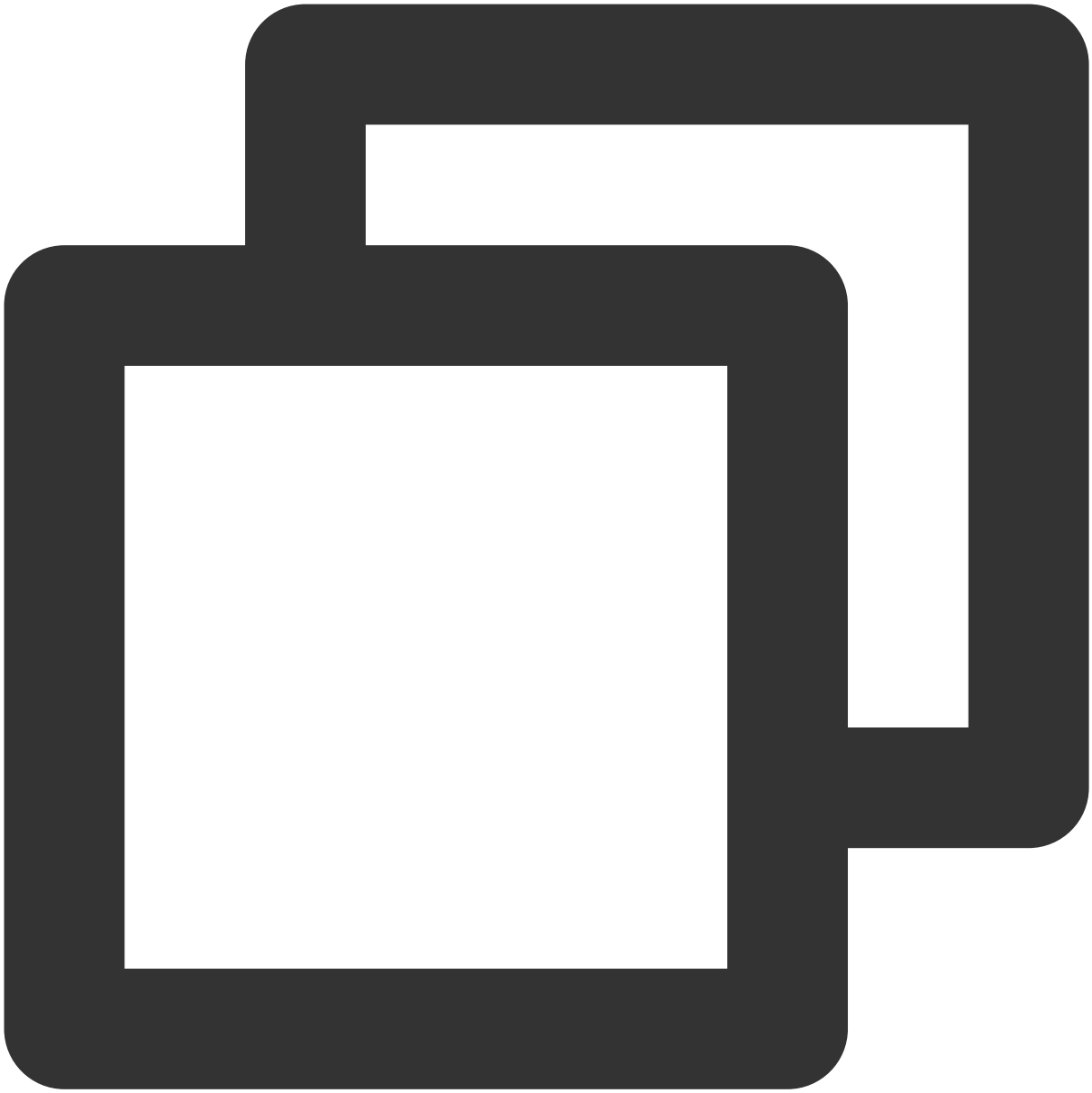
1. Masuk ke CVM gateway publik, aktifkan penerusan jaringan dan proksi NAT, dan optimalkan parameter terkait.

1.1 Jalankan perintah berikut untuk membuat file bernama `vpcGateway.sh` di `usr/local/sbin` .



```
vim /usr/local/sbin/vpcGateway.sh
```

1.2 Tekan **i** (i) untuk masuk ke mode edit dan tambahkan kode berikut ke dalam skrip:

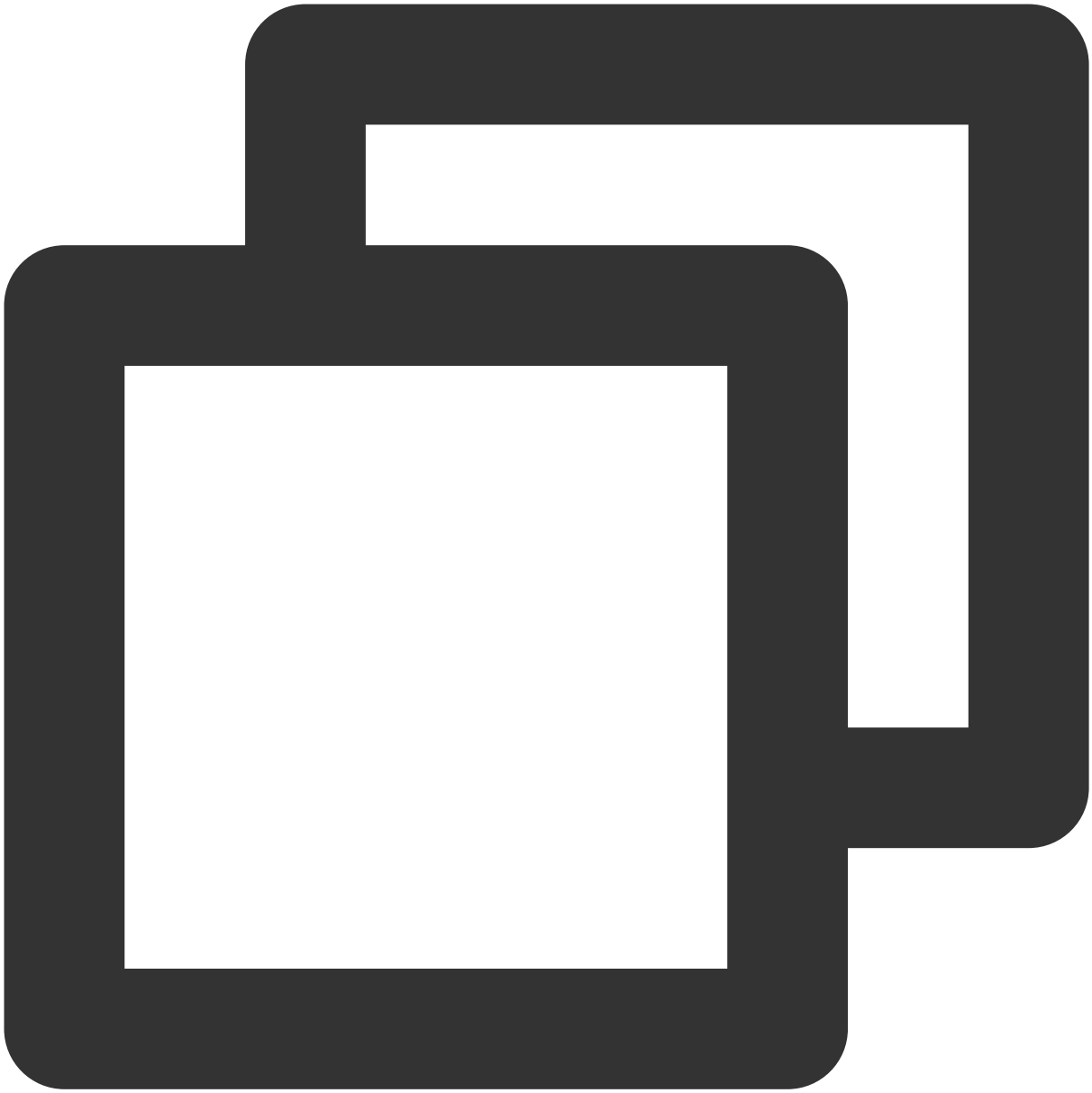


```
#!/bin/bash
echo "------------------------------------------------"
echo "          `date`"
echo "(1)ip_forward config......"
file="/etc/sysctl.conf"
grep -i "^net\\.ipv4\\.ip_forward.*" $file &>/dev/null && sed -i \\
's/net\\.ipv4\\.ip_forward.*/net\\.ipv4\\.ip_forward = 1/' $file || \\
echo "net.ipv4.ip_forward = 1"  >> $file
echo 1 >/proc/sys/net/ipv4/ip_forward
[ `cat /proc/sys/net/ipv4/ip_forward` -eq 1 ] && echo "-->ip_forward:Success" || \\
echo "-->ip_forward:Fail"
```

```
echo "(2)Iptables set......"
iptables -t nat -A POSTROUTING -j MASQUERADE && echo "-->nat:Success" || echo "-->n
iptables -t mangle -A POSTROUTING -p tcp -j TCPOPTSTRIP --strip-options timestamp &
echo "-->mangle:Success" || echo "-->mangle:Fail"
echo "(3)nf_conntrack config......"
echo 262144 >  /sys/module/nf_conntrack/parameters/hashsize
[ `cat /sys/module/nf_conntrack/parameters/hashsize` -eq 262144 ] && \\
echo "-->hashsize:Success" ||  echo "-->hashsize:Fail"
echo 1048576 > /proc/sys/net/netfilter/nf_conntrack_max
[ `cat /proc/sys/net/netfilter/nf_conntrack_max` -eq 1048576 ] && \\
echo  "-->nf_conntrack_max:Success" ||  echo  "-->nf_conntrack_max:Fail"
echo 10800 >/proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established \\
[ `cat /proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established` -eq 10800 ] \\
&& echo  "-->nf_conntrack_tcp_timeout_established:Success" ||  \\
echo  "-->nf_conntrack_tcp_timeout_established:Fail"
```

1.3 Tekan **Esc** (Esc) untuk keluar dari mode edit dan masukkan **:wq** (:wq) untuk menyimpan file dan kembali.

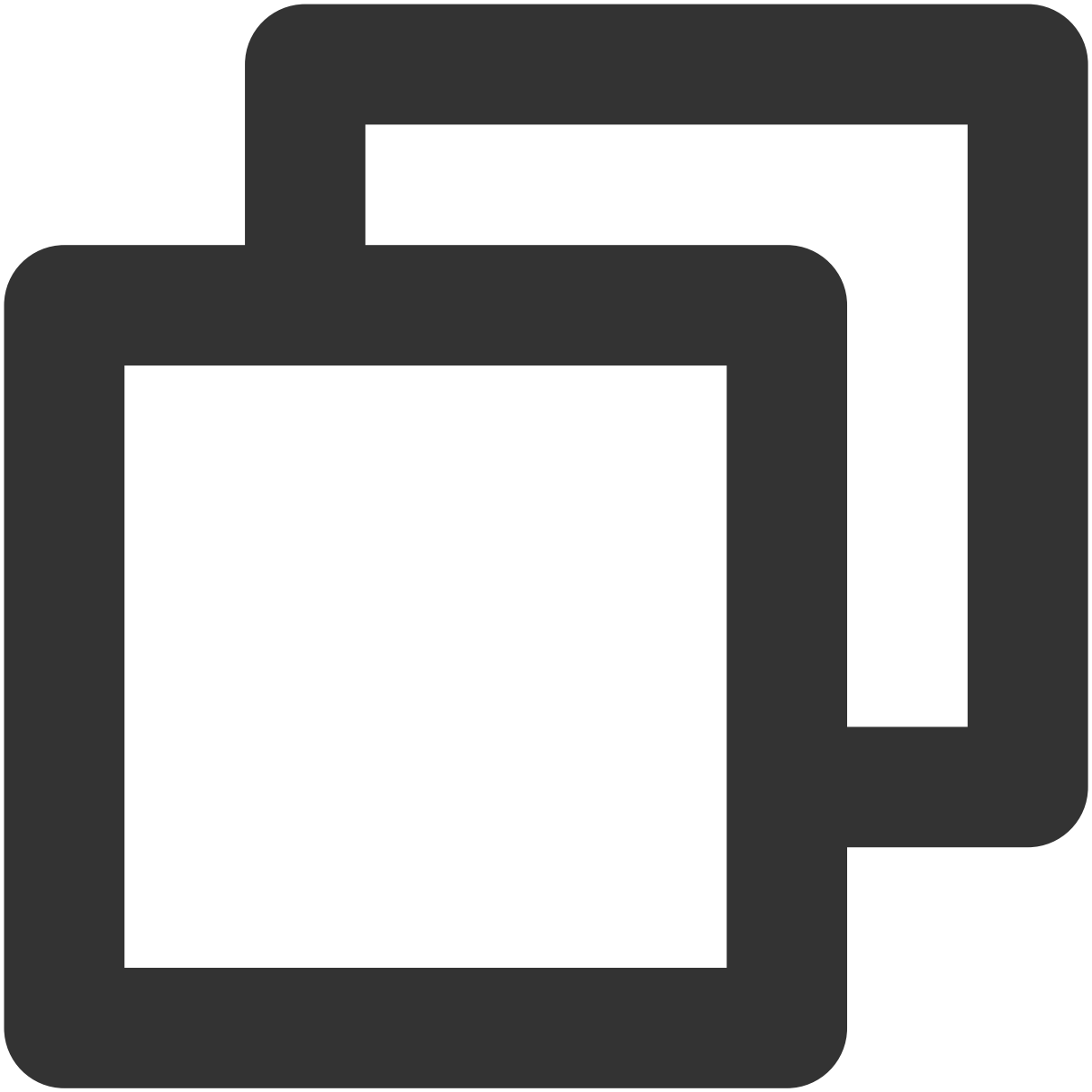
Kemudian, jalankan perintah berikut:



```
chmod +x /usr/local/sbin/vpcGateway.sh
echo "/usr/local/sbin/vpcGateway.sh  >/tmp/vpcGateway.log 2>&1" >> /etc/rc.local
```

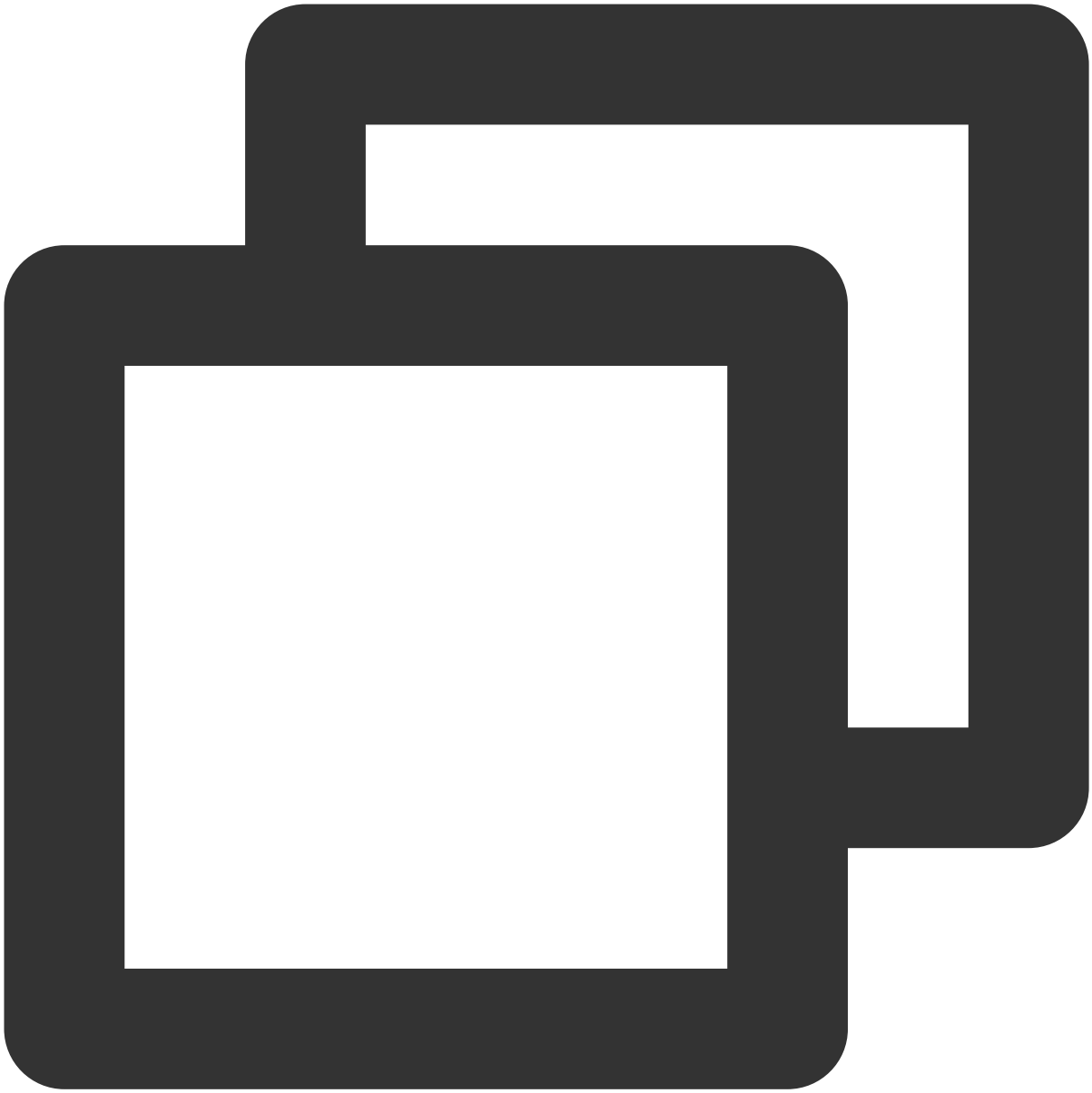
2. Atur RPS gateway publik.

2.1 Jalankan perintah berikut untuk membuat file bernama `setrps.sh` di `usr/local/sbin` .



```
vim /usr/local/sbin/set_rps.sh
```

2.2 Tekan **i** (i) untuk masuk ke mode edit dan tambahkan kode berikut ke dalam skrip:

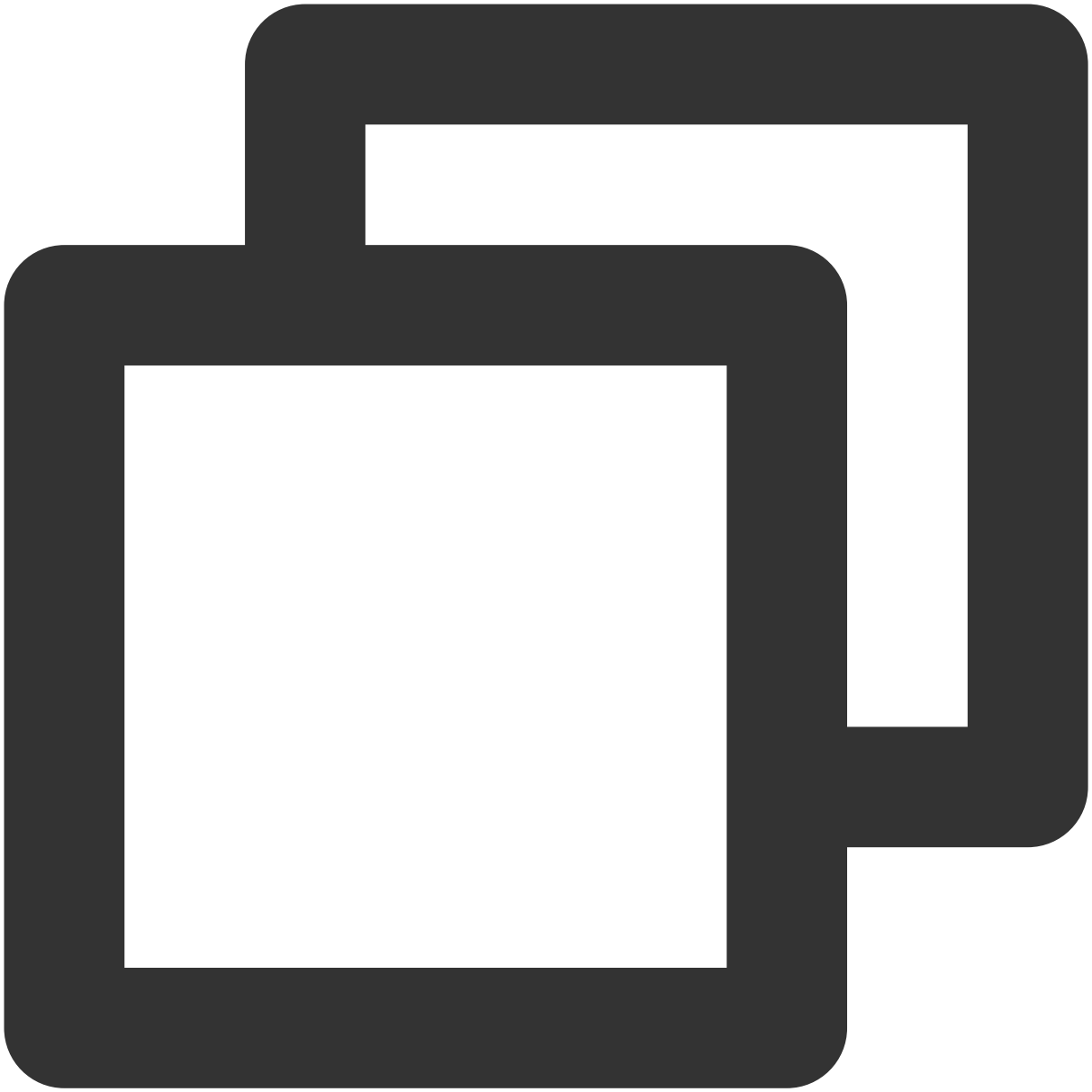


```
#!/bin/bash
echo "----------------------------------------"
* date
mask=0
i=0
total_nic_queues=0

get_all_mask() {
        local cpu_nums=$1
        if [ $cpu_nums -gt 32 ]; then
                mask_tail=""
```

```
                mask_low32="ffffffff"
                idx=$((cpu_nums / 32))
                cpu_reset=$((cpu_nums - idx * 32))

                if [ $cpu_reset -eq 0 ]; then
                        mask=$mask_low32
                        for ((i = 2; i <= idx; i++)); do
                                mask="$mask,$mask_low32"
                        done
                else
                    for ((i = 1; i <= idx; i++)); do
                        mask_tail="$mask_tail,$mask_low32"
                done
                mask_head_num=$((2 ** cpu_reset - 1))
                mask=$(printf "%x%s" $mask_head_num $mask_tail)
            fi
        else
            mask_num=$((2 ** cpu_nums - 1))
            mask=$(printf "%x" $mask_num)
        fi
        echo $mask
}
set_rps() {
      if ! command -v ethtool &>/dev/null; then
        source /etc/profile
      fi

      ethtool=$(which ethtool)

      cpu_nums=$(cat /proc/cpuinfo | grep processor | wc -l)
      if [ $cpu_nums -eq 0 ]; then
          exit 0
      fi

      mask=$(get_all_mask $cpu_nums)
      echo "cpu number:$cpu_nums  mask:0x$mask"

      ethSet=$(ls -d /sys/class/net/eth*)

      for entry in $ethSet; do
          eth=$(basename $entry)
          nic_queues=$(ls -l /sys/class/net/$eth/queues/ | grep rx- | wc -l)
          if (($nic_queues == 0)); then
              continue
          fi

          cat /proc/interrupts | grep "LiquidIO.*rxtx" &>/dev/null
```

```
            if [ $? -ne 0 ]; then # not smartnic
                #multi queue don't set rps
                max_combined=$(
                    $ethtool -l $eth 2>/dev/null | grep -i "combined" | head -n 1 | a
                )
                #if ethtool -l $eth goes wrong.
                [[ ! "$max_combined" =~ ^[0-9]+$ ]] && max_combined=1
                if [ ${max_combined} -ge ${cpu_nums} ]; then
                    echo "$eth has equally nic queue as cpu, don't set rps for it..."
                    continue
                fi
            else
               echo "$eth is smartnic, set rps for it..."
            fi

            echo "eth:$eth antrian:$nic_queues"
            total_nic_queues=$(($total_nic_queues + $nic_queues))
            i=0
            while (($i < $nic_queues)); do
                echo $mask >/sys/class/net/$eth/queues/rx-$i/rps_cpus
                echo 4096 >/sys/class/net/$eth/queues/rx-$i/rps_flow_cnt
                  i=$(($i + 1))
           done
       done

       flow_entries=$((total_nic_queues * 4096))
       echo "total_nic_queues:$total_nic_queues  flow_entries:$flow_entries"
       echo $flow_entries >/proc/sys/net/core/rps_sock_flow_entries
}
set_rps
```

2.3 Tekan **Esc** (Esc) untuk keluar dari mode edit dan masukkan **:wq** (:wq) untuk menyimpan file dan kembali. Kemudian, jalankan perintah berikut:



```
chmod +x /usr/local/sbin/set_rps.sh
echo "/usr/local/sbin/set_rps.sh >/tmp/setRps.log 2>&1" >> /etc/rc.local
```

3. Boot ulang CVM gateway untuk menerapkan konfigurasi. Kemudian, uji apakah CVM yang tidak memiliki IP publik dapat mengakses Internet melalui CVM gateway publik.

# Koneksi Langsung EIP

Waktu update terbaru：2022-10-11 14:14:13

## Kasus Penggunaan

Saat ingin mengakses Internet melalui EIP, Anda dapat memilih mode NAT atau mode koneksi langsung. Mode default adalah mode NAT.
Dalam mode NAT, EIP tidak terlihat di mesin lokal.
Dalam mode koneksi langsung, EIP terlihat di mesin lokal. Anda tidak perlu menambahkan alamat EIP secara manual untuk setiap konfigurasi, yang dapat meminimalkan biaya pengembangan.
Mode NAT dapat memenuhi sebagian besar persyaratan. Namun, jika ingin memeriksa IP publik pada CVM, Anda perlu menggunakan mode koneksi langsung EIP.

## Batasan Penggunaan

Saat ini, koneksi langsung EIP sedang dalam pengujian beta dan hanya tersedia untuk pengguna yang diizinkan. Koneksi ini hanya mendukung perangkat di VPC. Anda dapat kirim tiket untuk mengajukan fitur ini.
Gateway NAT dapat diikat dengan EIP yang diaktifkan dengan koneksi langsung, tetapi koneksi langsung tidak dapat diimplementasikan.
Pada CVM, koneksi langsung EIP tidak dapat diterapkan bersamaan dengan gateway NAT. Jika tabel perutean yang terkait dengan subnet tempat CVM Anda berada dikonfigurasi dengan kebijakan perutean mengakses jaringan publik melalui gateway NAT, koneksi langsung tidak dapat diimplementasikan melalui EIP pada CVM. Anda dapat mengizinkan CVM mengakses jaringan publik melalui EIP-nya dengan menyesuaikan prioritas gateway NAT dan EIP. Dalam hal ini, koneksi langsung EIP dapat diimplementasikan.

## Petunjuk

Untuk menggunakan koneksi langsung EIP, Anda harus mengaktifkannya di konsol dan menambahkan IP ke ENI di sistem operasi. Anda juga perlu mengonfigurasi perutean di sistem operasi sesuai dengan aplikasi Anda. Oleh karena itu, kami menyediakan skrip untuk mengonfigurasi IP agar lalu lintas jaringan pribadi melewati IP pribadi dan lalu lintas jaringan publik melewati IP publik.
**Keterangan:**
Untuk aplikasi lain, konfigurasikan perutean yang sesuai.

### Mengonfigurasi koneksi langsung EIP di CVM Linux

**Keterangan:**

Skrip untuk Linux mendukung CentOS 6 dan yang lebih baru, serta Ubuntu.

Skrip untuk Linux hanya mendukung ENI primer (eth0) dan tidak mendukung ENI sekunder.

Jika IP publik yang terikat ke ENI primer bukan EIP, Anda perlu mengonversi IP publik ke EIP. Untuk informasi selengkapnya, lihat Mengonversi IP publik ke EIP.

**Skenario**

Skrip untuk Linux berlaku untuk skenario berikut: IP pribadi dan IP publik keduanya terikat ke ENI primer (eth0), tempat alamat jaringan publik diakses melalui IP publik, dan alamat jaringan privat diakses melalui IP pribadi.

**Langkah 1: unduh skrip untuk koneksi langsung EIP**

Koneksi langsung EIP dapat menyebabkan gangguan jaringan. Dengan demikian, Anda perlu mengunduh skrip untuk koneksi langsung EIP dan mengunggahnya ke CVM terlebih dahulu. Anda dapat memperoleh skrip dengan menggunakan salah satu metode berikut:

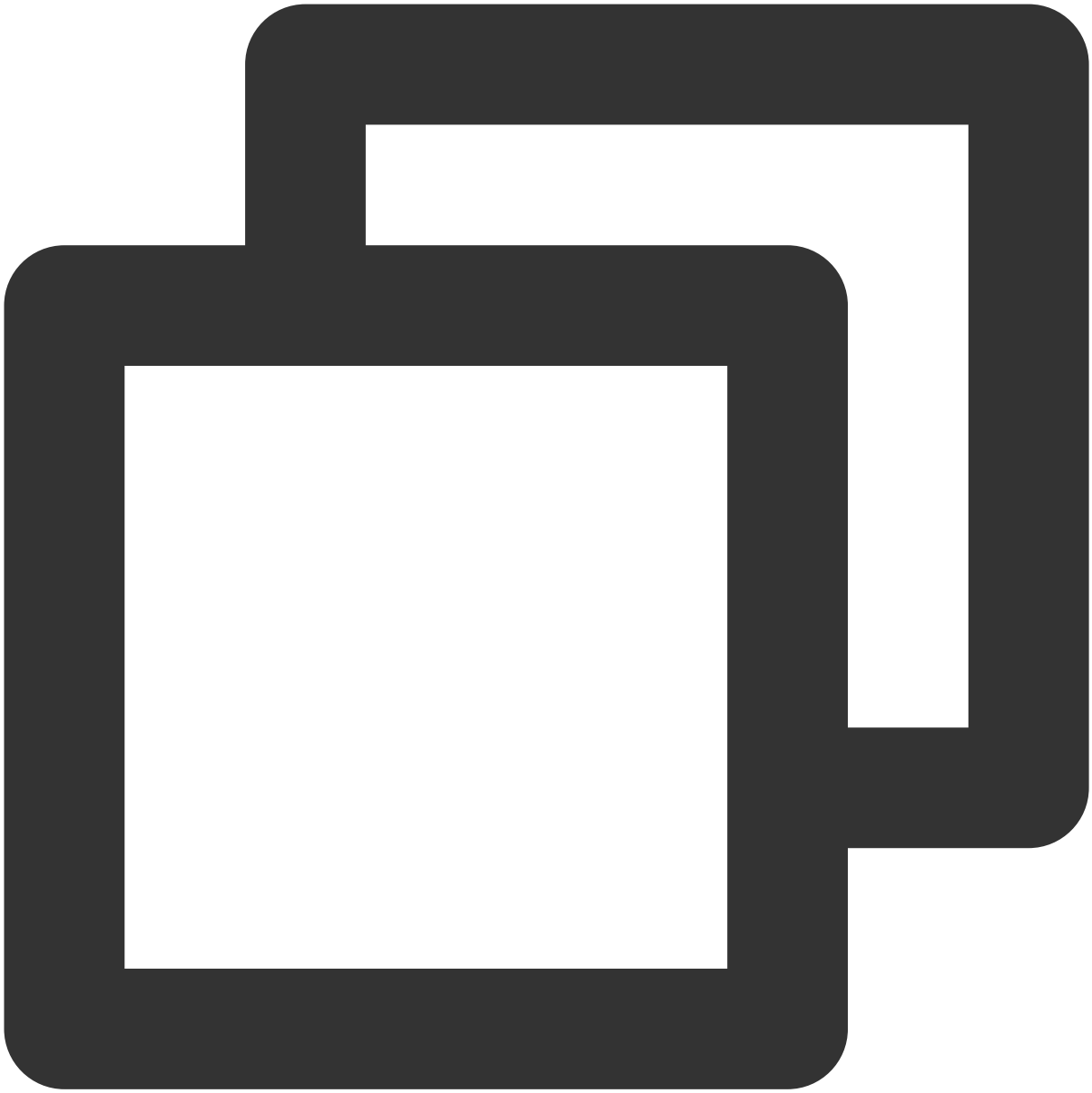
**Method 1: upload the script for EIP direct connection** (Metode 1: Unggah skrip untuk koneksi langsung EIP)

(1) Unduh skrip konfigurasi untuk koneksi langsung EIP dari Unduh Script untuk Linux

(2) Setelah skrip untuk Linux diunduh ke mesin lokal, unggah ke CVM yang memerlukan koneksi langsung EIP.

**Method 2: directly use a command** (Metode 2: langsung gunakan perintah)

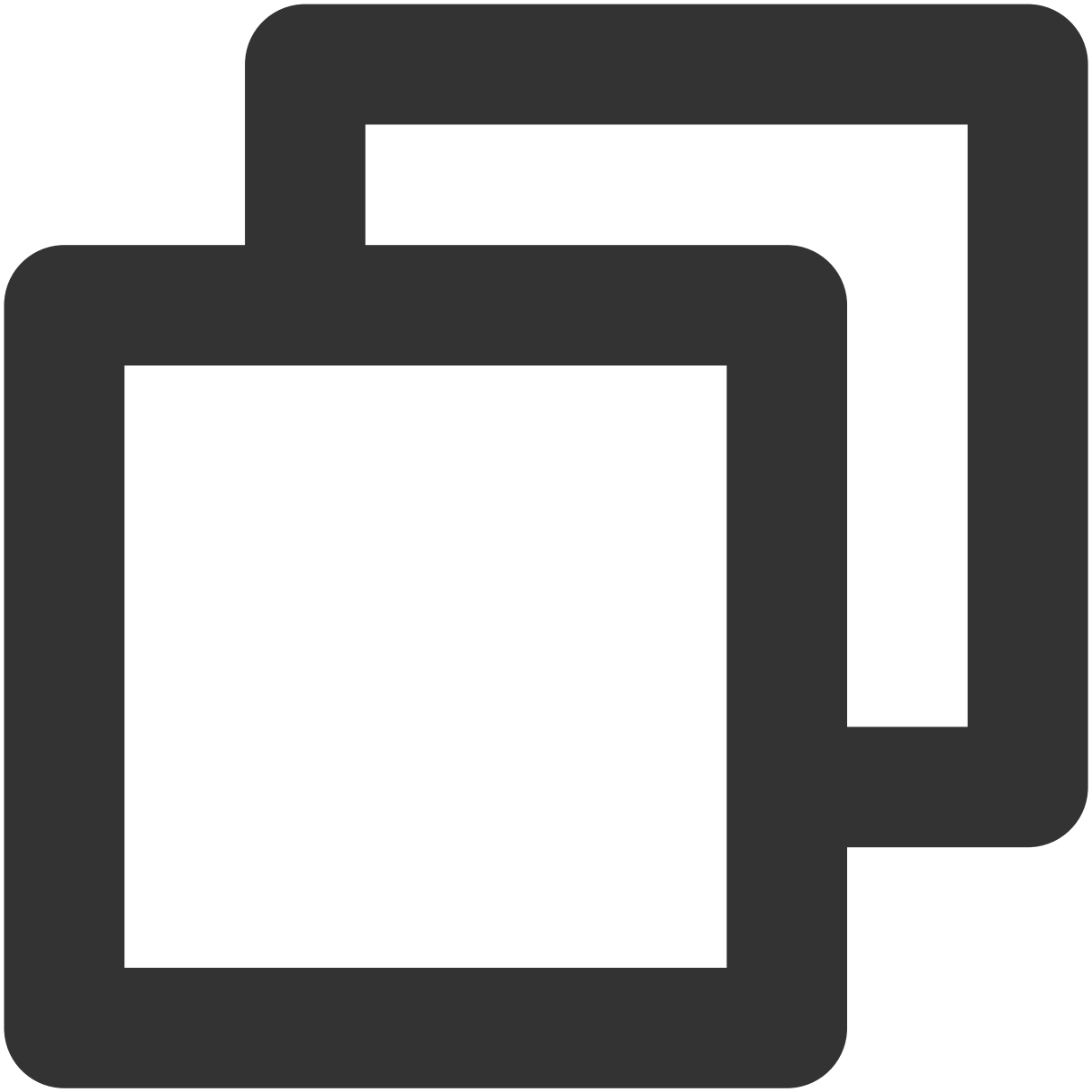
Login ke CVM, dan jalankan perintah berikut pada CVM untuk mengunduh skrip:



```
wget https://network-data-1255486055.cos.ap-guangzhou.myqcloud.com/eip_direct.sh
```

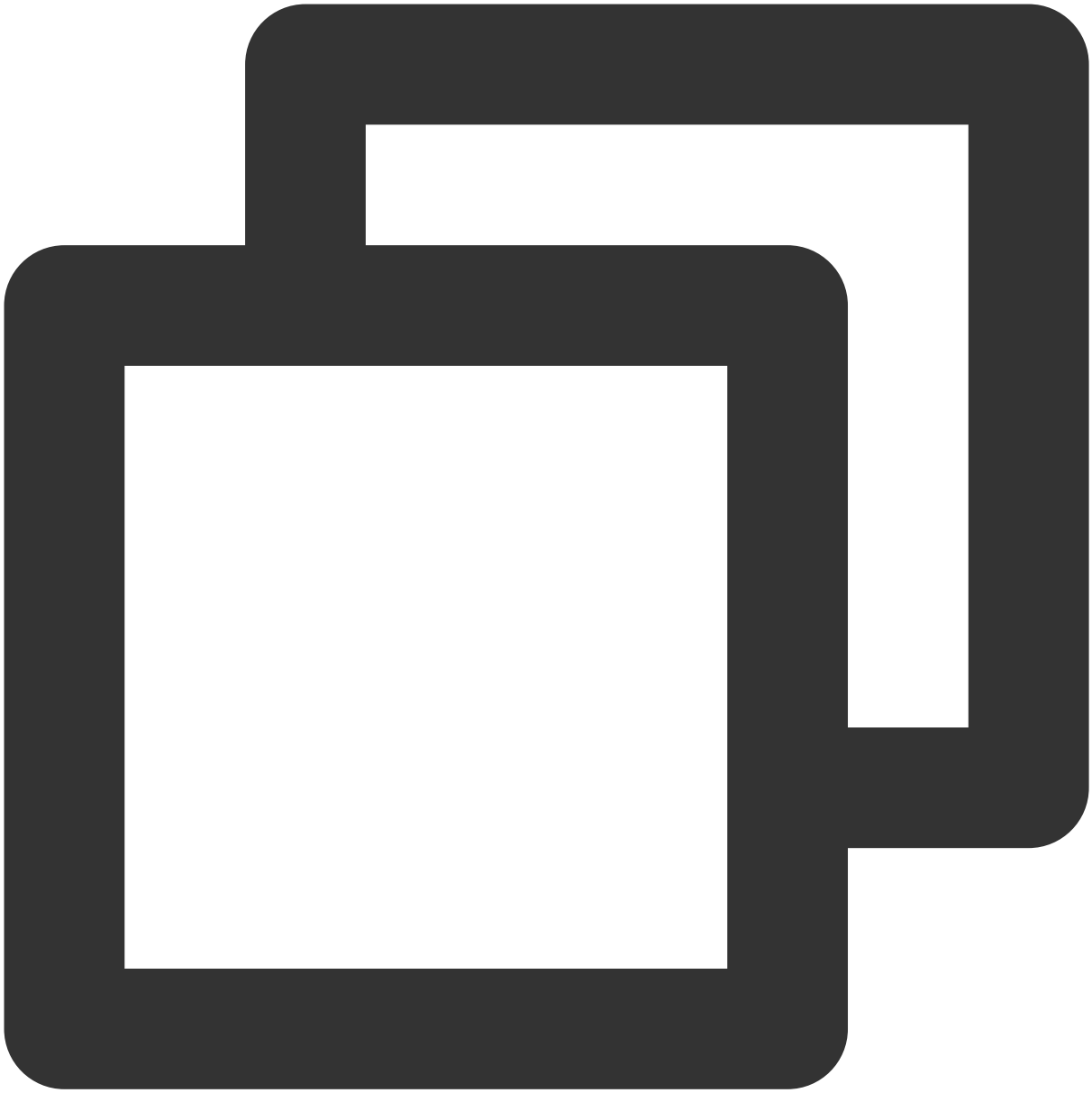
**Langkah 2: jalankan skrip untuk koneksi langsung EIP**

1. Login ke CVM yang memerlukan koneksi langsung EIP.
2. Jalankan skrip untuk koneksi langsung EIP sebagai berikut:
(1) Jalankan perintah berikut untuk menambahkan izin eksekusi:



```
chmod +x eip_direct.sh
```

(2) Jalankan perintah berikut untuk menjalankan skrip:



```
./eip_direct.sh install XX.XX.XX.XX
```

Di sini, XX.XX.XX.XX menunjukkan alamat EIP (opsional). Anda dapat membiarkannya kosong dan menjalankan `./eip_direct.sh install` secara langsung.

**Langkah 3: aktifkan koneksi langsung EIP**

1. Login ke Konsol EIP.
2. Temukan EIP target, dan pilih **More** (Lainnya) -> **Direct connection** (Koneksi langsung) di kolom **Operation** (Operasi) di sebelah kanan.

## Mengonfigurasi koneksi langsung EIP pada CVM Windows

**Keterangan:**

Untuk menggunakan koneksi langsung EIP di Windows, Anda memerlukan satu ENI untuk IP pribadi dan satu ENI untuk IP publik, lalu ikat IP publik ke ENI primer dan ikat IP pribadi ke ENI sekunder.

Selama konfigurasi koneksi langsung EIP di Windows, koneksi internet Anda bisa saja terputus. Dengan demikian, sebaiknya login ke instans Windows melalui VNC.

Jika IP publik yang terikat ke ENI primer bukan EIP, Anda perlu mengonversi IP publik ke EIP. Untuk informasi selengkapnya, lihat Mengonversi IP publik ke EIP.

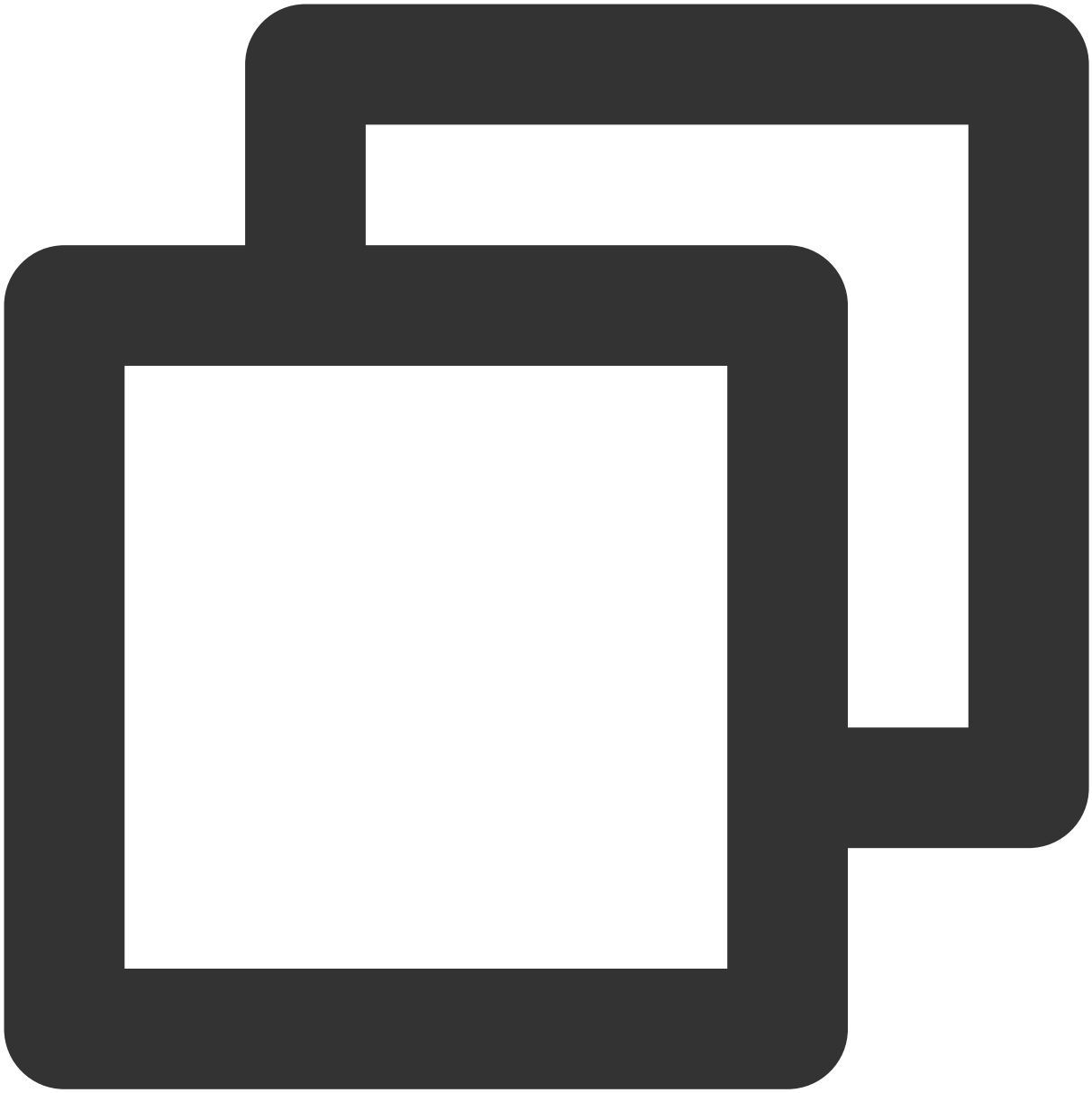
### Skenario

Skrip untuk Windows berlaku untuk skenario berikut ini: Lalu lintas jaringan publik melewati ENI primer, dan lalu lintas jaringan pribadi melewati ENI sekunder.

### Langkah 1: unduh skrip untuk koneksi langsung EIP

Selama konfigurasi koneksi langsung EIP, koneksi internet akan terganggu. Dengan demikian, Anda perlu mengunduh skrip untuk koneksi langsung EIP dan mengunggahnya ke CVM terlebih dahulu.

Buka tautan berikut di browser CVM untuk mengunduh skrip untuk koneksi langsung EIP:



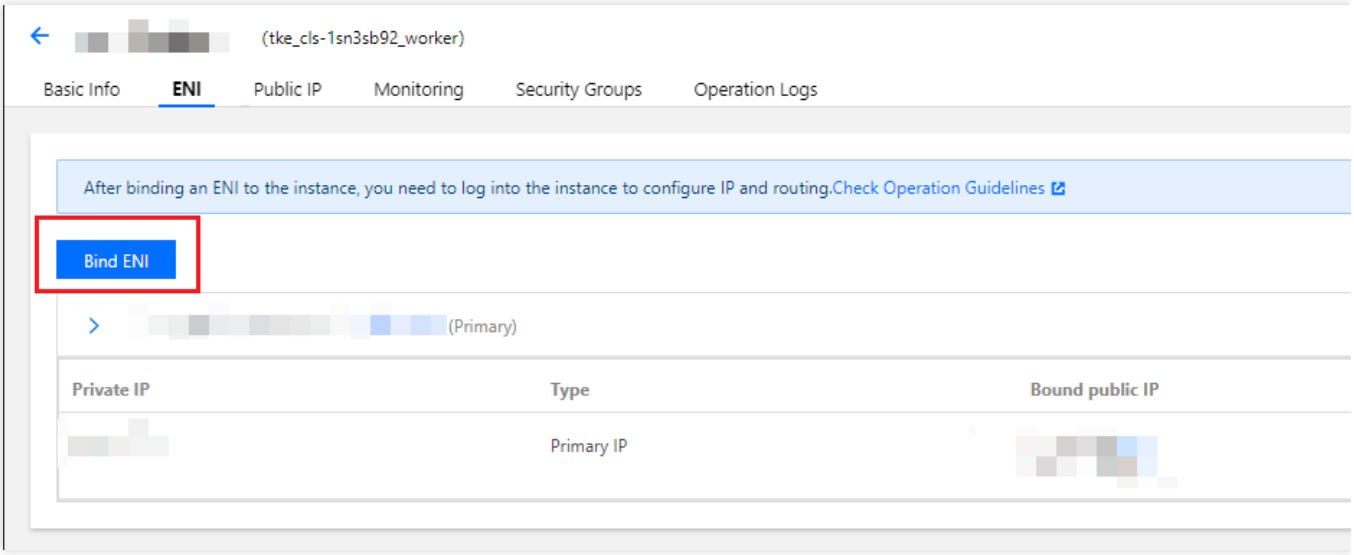
```
https://windows-1254277469.cos.ap-guangzhou.myqcloud.com/eip_windows_direct.bat
```

**Langkah 2: konfigurasikan ENI sekunder**

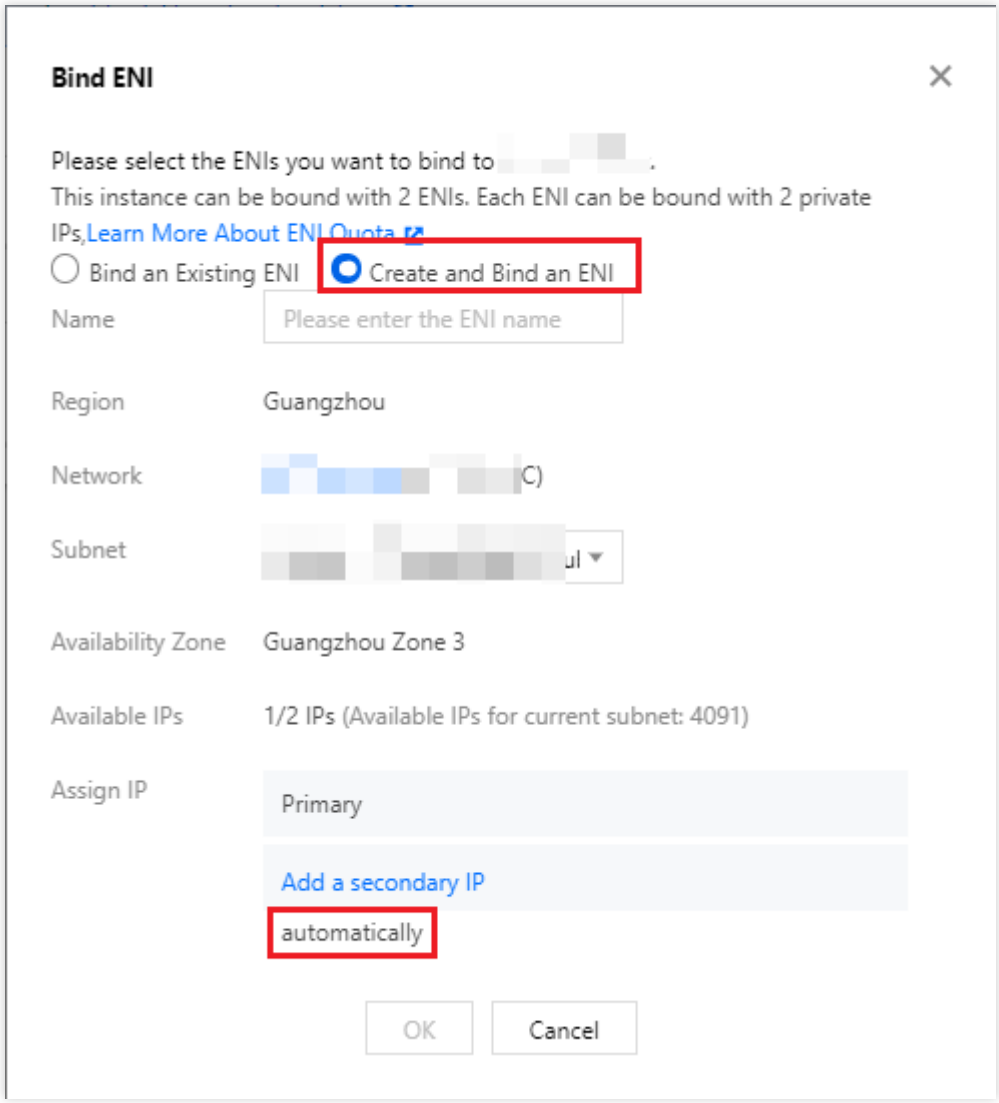
1. Login ke Konsol CVM.

2. Pada halaman **Instances** (Instans), klik CVM ID yang dikonfigurasi untuk membuka halaman **Basic Information** (Informasi Dasar).

3. Pilih tab **ENI** (ENI), lalu klik **Bind ENI** (Ikat ENI) untuk membuat ENI yang berada di subnet yang sama dengan ENI primer.




4. Di jendela pop-up, pilih **Create and Bind an ENI** (Buat dan Ikat ENI), masukkan informasinya, pilih **Automatic Assignment** (Penetapan Otomatis) di bagian **Assign IP** (Tetapkan IP) dan klik **OK** (OKE).




**Langkah 3: konfigurasikan koneksi langsung EIP untuk ENI primer**

1. Login ke Konsol EIP.

2. Temukan EIP yang terikat ke ENI primer dan pilih **More** (Lainnya) -> **Direct Connection** (Koneksi Langsung) di kolom **Operation** (Operasi) di sebelah kanan.

**Langkah 4: konfigurasikan IP di CVM**

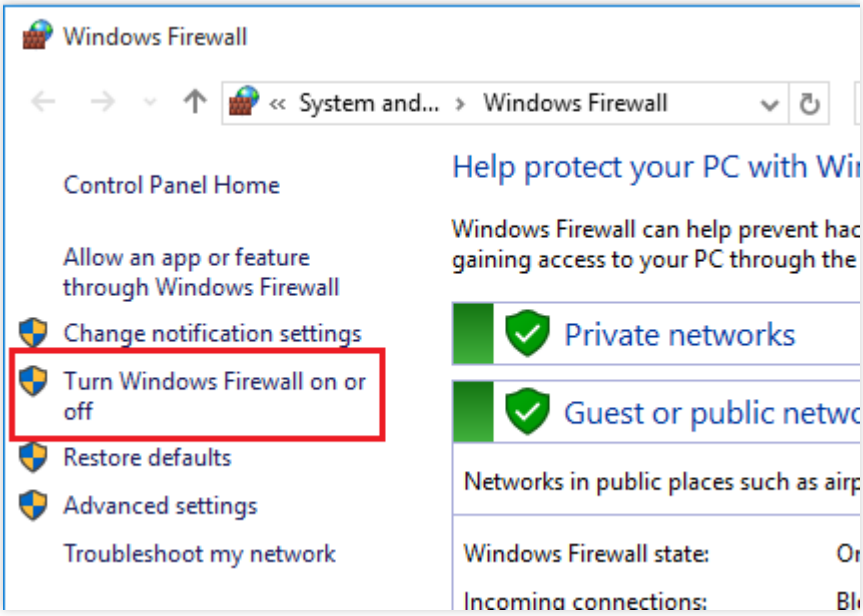
1. Login ke CVM. Operasi ini dapat menyebabkan gangguan jaringan publik. Dengan demikian, Anda perlu Login ke instans Windows melalui VNC.

2. Pada halaman sistem operasi, pilih

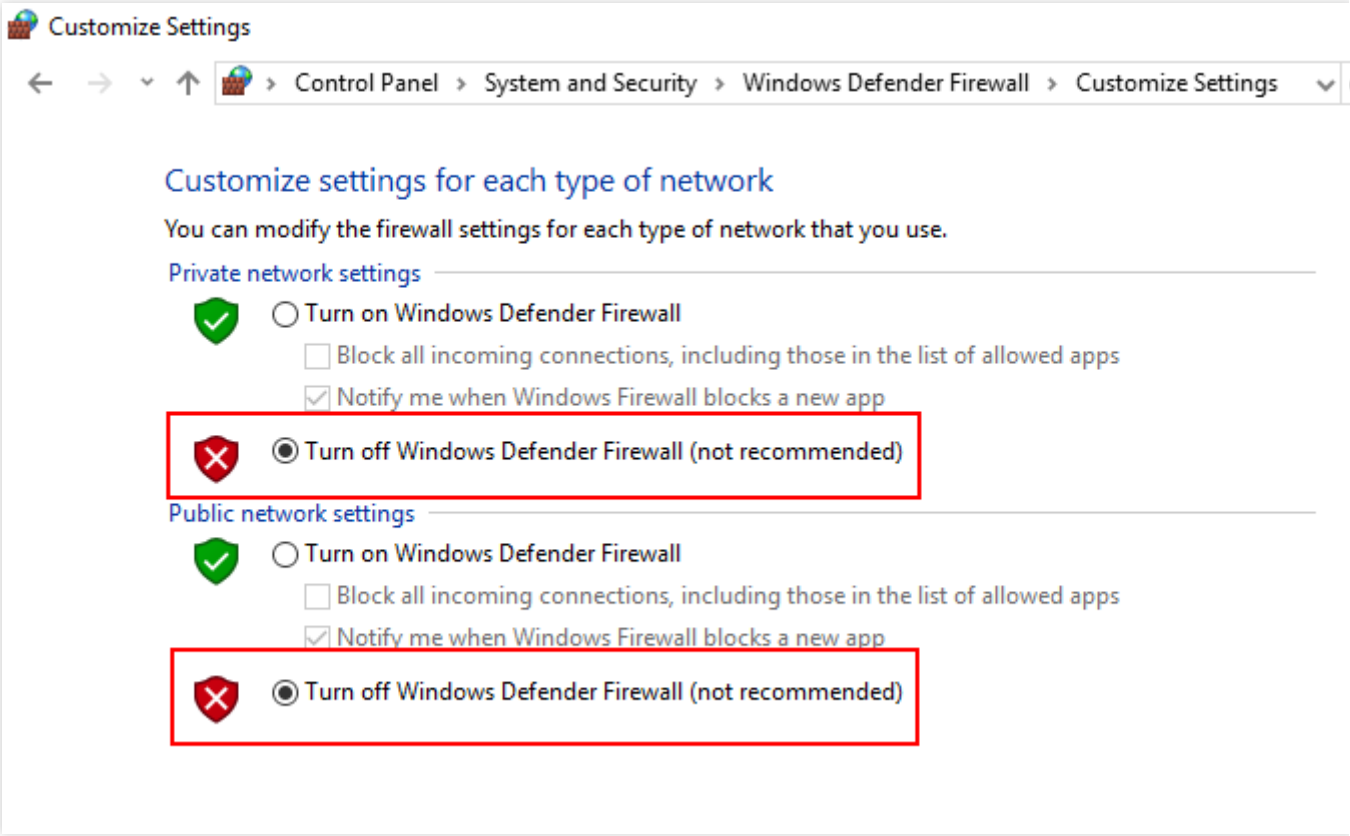
di pojok kiri bawah dan klik

untuk membuka jendela **Windows PowerShell** (Windows PowerShell). Masukkan `firewall.cpl` , lalu tekan Enter untuk membuka halaman **Windows Firewall** (Windows Firewall).

3. Klik **Turn Windows Firewall on or off** (Aktifkan atau nonaktifkan Windows Firewall) untuk membuka halaman **Customize Settings** (Sesuaikan Pengaturan).




4. Pilih **Turn off Windows Firewall** (Nonaktifkan Windows Firewall) baik di panel **Private network settings** (Pengaturan jaringan pribadi) dan panel **Public network settings** (Pengaturan jaringan publik).




5. Klik dua kali untuk menjalankan skrip yang diunduh di Langkah 1. Masukkan alamat IP publik dan tekan Enter dua kali.

6. Masukkan `ipconfig` di jendela **Windows PowerShell** (Windows PowerShell), lalu tekan Enter. Anda dapat melihat bahwa alamat IPv4 pada ENI primer akan berubah menjadi alamat jaringan publik.

**Keterangan:**

Saat koneksi langsung diaktifkan, Anda tidak dapat menetapkan IP pribadi ke ENI primer. Jika tidak, CVM tidak dapat mengakses jaringan publik.

# Keamanan
# Grup Keamanan
# Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:47

Grup keamanan adalah firewall virtual yang menampilkan pemfilteran paket data stateful. Ini digunakan untuk mengonfigurasi kontrol akses jaringan CVM, Cloud Load Balancer, TencentDB, dan instans lainnya sambil mengontrol lalu lintas keluar dan masuknya. Ini adalah sarana penting untuk isolasi keamanan jaringan.
Anda dapat mengonfigurasi aturan grup keamanan untuk mengizinkan atau menolak lalu lintas masuk dan keluar instans dalam grup keamanan.

## Fitur Grup Keamanan

Grup keamanan adalah grup logis. Anda dapat menambahkan CVM, ENI, TencentDB, dan instans lainnya di wilayah yang sama dengan persyaratan isolasi keamanan jaringan yang sama ke grup keamanan yang sama.
Secara default, instans dalam grup keamanan yang sama tidak saling berhubungan, kecuali jika Anda mengizinkannya dengan menetapkan aturan.
Grup keamanan bersifat stateful. Lalu lintas masuk yang Anda izinkan dapat secara otomatis menjadi keluar dan sebaliknya.
Anda dapat mengubah aturan grup keamanan kapan saja, dan aturan baru akan segera berlaku.

## Batasan Penggunaan

Untuk informasi selengkapnya tentang batas penggunaan dan kuota grup keamanan, lihat **security group limits** (batas grup keamanan) di Ikhtisar Batas Penggunaan.

## Aturan Grup Keamanan

### Komponen

Aturan grup keamanan terdiri dari:
Sumber: Alamat IP data sumber (masuk) atau data target (keluar).
Jenis protokol dan port protokol: jenis protokol, seperti TCP, UDP, dll.
Kebijakan: mengizinkan atau menolak permintaan akses.

### Prioritas aturan

Aturan dalam grup keamanan diprioritaskan dari atas ke bawah. Aturan di bagian atas daftar memiliki prioritas tertinggi dan akan berlaku lebih dahulu, sedangkan aturan di bagian bawah memiliki prioritas terendah dan akan berlaku terakhir.
Jika ada konflik aturan, aturan dengan prioritas lebih tinggi akan berlaku secara default.
Saat lalu lintas masuk atau keluar dari instans yang terikat ke grup keamanan, aturan grup keamanan akan dicocokkan secara berurutan dari atas ke bawah. Jika aturan berhasil dicocokkan dan berlaku, aturan berikutnya tidak akan cocok.

### Beberapa grup keamanan

Instans dapat diikat ke satu atau beberapa grup keamanan. Ketika terikat ke beberapa grup keamanan, aturan grup keamanan akan dicocokkan secara berurutan dari atas ke bawah. Anda dapat menyesuaikan prioritas grup keamanan kapan saja.

## Templat Grup Keamanan

Saat membuat grup keamanan, Anda dapat memilih salah satu dari dua templat grup keamanan yang disediakan oleh Tencent Cloud:
Templat yang membuka semua port: semua lalu lintas masuk dan keluar akan diizinkan untuk diteruskan.
Templat yang membuka port utama: port TCP 22 (untuk login SSH Linux), port 80 dan 443 (untuk Layanan web), port 3389 (untuk login jarak jauh Windows), protokol ICMP (untuk Perintah ping), dan jaringan pribadi akan terbuka untuk Internet.
**Keterangan:**
Jika templat ini tidak dapat memenuhi kebutuhan aktual Anda, Anda dapat membuat grup keamanan kustom. Untuk informasi selengkapnya, lihat Membuat Grup Keamanan dan Kasus Penggunaan Grup Keamanan.
Jika Anda perlu melindungi lapisan aplikasi (HTTP/HTTPS), harap aktifkan Tencent Cloud Web Application Firewall (WAF), yang menyediakan keamanan web pada lapisan aplikasi untuk melindungi dari kerentanan web, perayap berbahaya, dan serangan CC, sehingga membantu melindungi situs web dan aplikasi web Anda.

## Cara Menggunakan Grup Keamanan

Gambar berikut menunjukkan cara menggunakan grup keamanan:


# Praktik Terbaik Grup Keamanan

### Membuat grup keamanan

Sebaiknya tentukan grup keamanan saat Anda membeli CVM melalui API. Jika tidak, grup keamanan default akan digunakan dan tidak dapat dihapus.
Jika Anda perlu mengubah kebijakan perlindungan instans, sebaiknya ubah aturan yang ada daripada membuat grup keamanan baru.

### Mengelola aturan

Ekspor dan cadangkan aturan grup keamanan sebelum Anda mengubahnya, sehingga Anda dapat mengimpor dan memulihkannya jika terjadi kesalahan.
Untuk membuat beberapa aturan grup keamanan, gunakan templat parameter.

### Mengaitkan grup keamanan

Anda dapat menambahkan instans dengan persyaratan perlindungan yang sama ke grup keamanan yang sama, sebagai ganti mengonfigurasi grup keamanan terpisah untuk setiap instans.
Sebaiknya jangan mengikat satu instans ke terlalu banyak grup keamanan, karena aturan dalam grup keamanan yang berbeda dapat bertentangan dan mengakibatkan pemutusan jaringan.

# Membuat Grup Keamanan

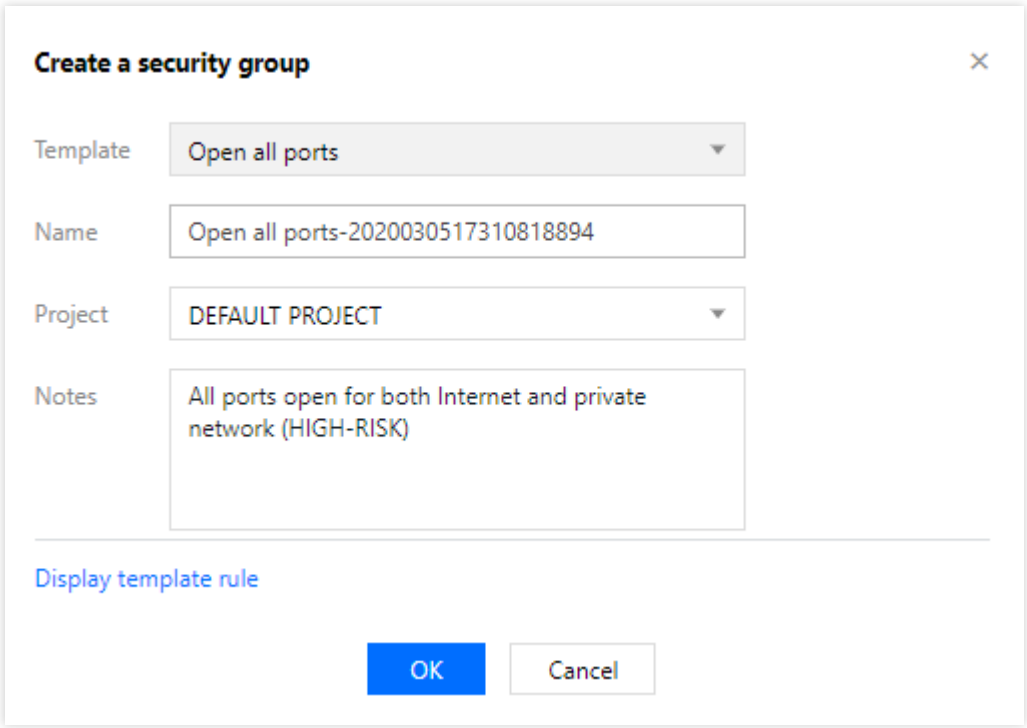
Waktu update terbaru：2021-12-20 15:52:35

## Skenario

Grup Keamanan bertindak sebagai firewall virtual untuk CVM. Setiap instans CVM harus dikaitkan dengan setidaknya satu grup keamanan. Secara default, setiap instans CVM memiliki dua templat (**Open all ports** (Buka semua port) dan **Open port 22, 80, 443, 3389 and ICMP protocol** (Buka port 22, 80, 443, 3389, dan protokol ICMP)) untuk membuat grup keamanan default. Untuk detailnya, lihat Ikhtisar Grup Keamanan.
Jika grup keamanan default tidak memenuhi kebutuhan Anda, Anda dapat membuat grup keamanan Anda sendiri seperti yang diinstruksikan di bawah ini.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah untuk grup keamanan. Klik **+New** (+Baru).
4. Di halaman **Create a security group** (Buat grup keamanan), selesaikan konfigurasi berikut:




**Template** (Templat): pilih templat yang sesuai dengan kebutuhan Anda, seperti yang ditampilkan di bawah ini:

| Templat | Deskripsi | Catatan |
| --- | --- | --- |
| Buka semua port | Semua port terbuka. Dapat menimbulkan masalah keamanan. | - |
| Buka port TCP 22, 80, 443, 3389, dan ICMP | Port TCP 22, 80, 443, dan 3389, dan ICMP terbuka. Semua port terbuka secara internal. | Cocok untuk instans dengan layanan web. |
| Kustom | Membuat grup keamanan kosong yang aturannya ditambahkan setelahnya. Untuk detail tentang cara menambahkan aturan, lihat artikel ini. | - |

**Name** (Nama): nama grup keamanan.

**Project** (Proyek): secara default, **Deafult project** (Proyek default) dipilih. Pilih proyek untuk manajemen yang lebih baik.

**Notes** (Catatan): deskripsi singkat untuk grup keamanan.

5. Klik **OK** (OKE) untuk membuat grup keamanan.

Jika Anda memilih **Custom** (Kustom) sebagai templat untuk grup keamanan Anda, klik **Add rules now** (Tambahkan aturan sekarang) untuk menambahkan aturan grup keamanan.

# Menambahkan Aturan Grup Keamanan

Waktu update terbaru：2022-07-11 16:44:08

## Ikhtisar

Grup keamanan digunakan untuk mengatur lalu lintas ke dan dari jaringan publik dan pribadi. Demi keamanan, sebagian besar lalu lintas masuk ditolak secara default. Jika Anda memilih **Open all ports** (Buka semua port) atau **Open ports 22, 80, 443, 3389 and ICMP protocol** (Buka port 22, 80, 443, 3389, dan protokol ICMP) sebagai templat saat membuat grup keamanan, aturan akan otomatis dibuat dan ditambahkan ke grup keamanan untuk mengizinkan lalu lintas di port tersebut. Untuk informasi selengkapnya, harap lihat Grup Keamanan.
Dokumen ini menjelaskan cara menambahkan aturan grup keamanan untuk mengizinkan atau menolak lalu lintas ke dan dari jaringan publik atau pribadi.

## Catatan

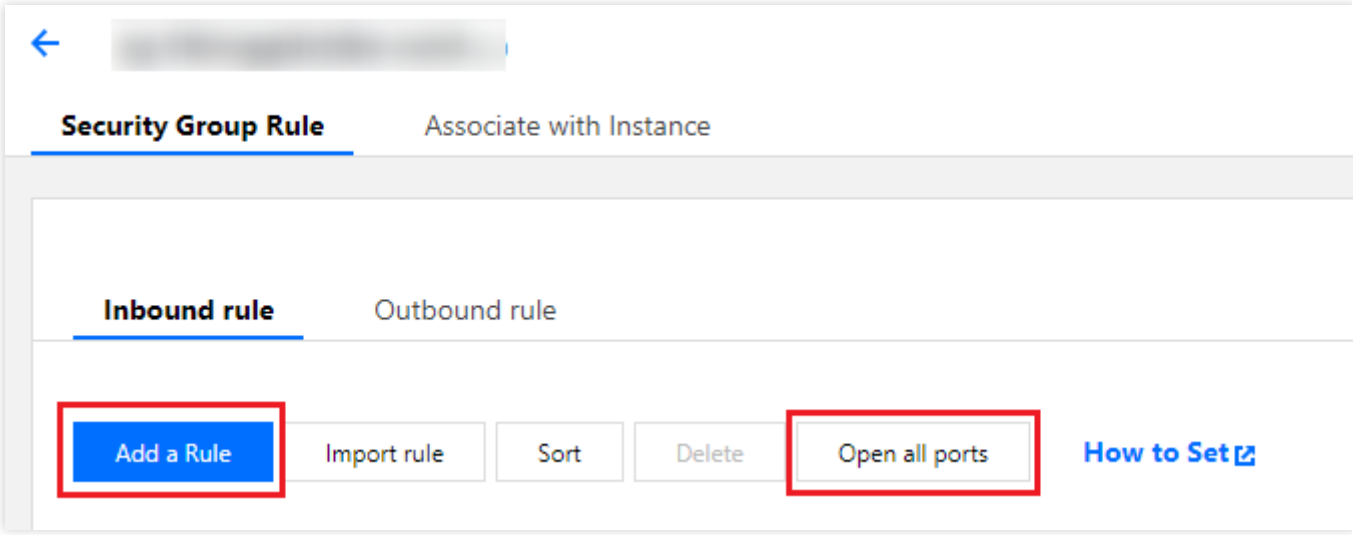
Aturan grup keamanan mendukung aturan IPv4 dan IPv6.
**Open all ports** (Buka semua port) mengizinkan lalu lintas IPv4 dan IPv6.

## Prasyarat

Anda harus memiliki grup keamanan yang ada. Jika tidak, lihat Membuat Grup Keamanan untuk detailnya.
Anda harus mengetahui lalu lintas mana yang diizinkan atau ditolak untuk instans CVM Anda. Untuk informasi selengkapnya tentang aturan grup keamanan dan kasus penggunaannya, harap lihat Kasus Penggunaan Grup Keamanan.

### Petunjuk

1. Login ke konsol CVM.
2. Pilih **Security Group (Grup Keamanan)** di bilah sisi kiri untuk mengakses halaman pengelolaan grup keamanan.
3. Pilih wilayah, dan temukan grup keamanan yang ingin Anda tetapkan aturannya.
4. Klik **Modify Rules** (Modifikasi Aturan) di kolom **Operation** (Operasi).
5.
Klik **Inbound rules**
(Aturan masuk) dan pilih salah satu metode berikut untuk menambahkan aturan.



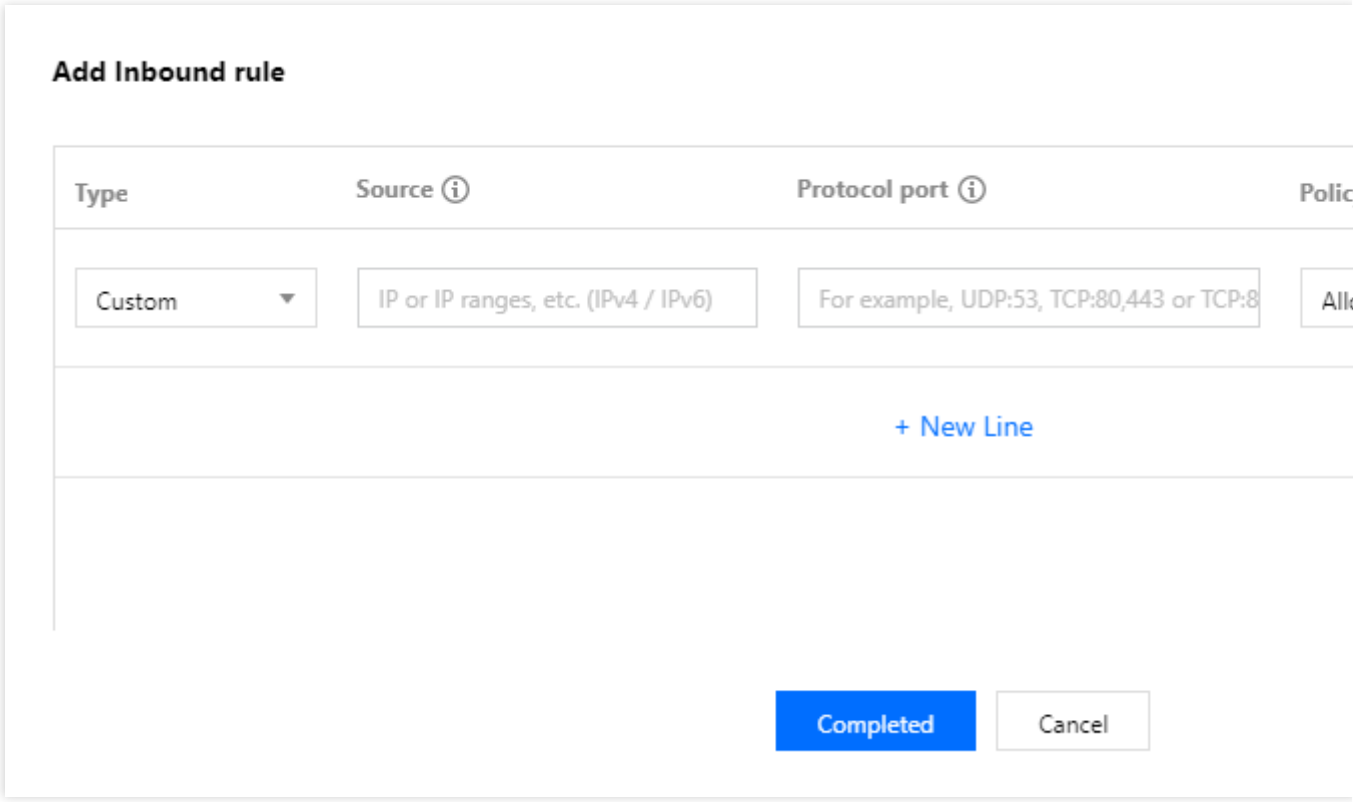

**Keterangan:**

Petunjuk berikut menggunakan **Add a Rule** (Tambahkan aturan) sebagai contoh.

**Open all ports** (Buka semua port): metode ini ideal jika Anda tidak memerlukan aturan ICMP kustom dan semua lalu lintas melewati port 20, 21, 22, 80, 443, dan 3389 dan protokol ICMP.

**Add a Rule** (Tambahkan Aturan): metode ini ideal jika Anda perlu menggunakan beberapa protokol dan port selain yang disebutkan di atas.

6. Di jendela pop-up, tetapkan aturan.




Konfigurasikan parameter berikut:

**Type** (Jenis): **Custom** (Kustom) dipilih secara default. Anda juga dapat memilih templat aturan sistem lain termasuk **Login Windows CVMs (3389)** (CVM Login Windows (3389)), **Login Linux CVMs (22)** (CVM Login Linux (22)), **Ping** (Ping), **HTTP (80)** (HTTP (80)), **HTTPS (443)** (HTTPS (443)), **MySQL (3306)** (MySQL (3306)), dan **SQL Server (1433)** (SQL Server (1433)).
**Source** (Sumber) atau **Destination** (Tujuan): sumber lalu lintas (aturan masuk) atau tujuan (aturan keluar). Anda perlu menentukan salah satu opsi berikut:

| Sumber atau Tujuan | Deskripsi |
| --- | --- |
| Satu alamat IPv4 atau rentang IPv4 | Dalam notasi CIDR, seperti `203.0.113.0`, `203.0.113.0/24` atau `0.0.0.0/0`, dimana `0.0.0.0/0` menunjukkan semua alamat IPv4 akan cocok. |
| Satu alamat IPv6 atau rentang IPv6 | Dalam notasi CIDR, seperti **FF05::B5**, `FF05:B5::/60`, `::/0` atau `0::0/0`, dimana `::/0` atau `0::0/0` menunjukkan semua alamat IPv6 akan dicocokkan. |
| ID grup keamanan yang dirujuk. Anda dapat merujuk ID dari:<br>Grup keamanan saat ini<br>Grup keamanan lainnya | Untuk merujuk grup keamanan saat ini, masukkan ID grup keamanan yang terkait dengan CVM.<br>Anda juga dapat merujuk grup keamanan lain di wilayah yang sama dan milik ke proyek yang sama dengan memasukkan ID grup keamanan.<br>**Keterangan:**<br>Grup keamanan yang dirujuk tersedia untuk Anda sebagai fitur lanjutan. Aturan grup keamanan yang dirujuk tidak ditambahkan ke grup keamanan saat ini.<br>Jika Anda memasukkan ID grup keamanan di Source (Sumber)/Destination (Tujuan) saat mengonfigurasi aturan grup keamanan, alamat IP pribadi instans CVM dan ENI yang terkait dengan ID grup keamanan ini akan digunakan sebagai sumber/tujuan. Hal ini tidak termasuk alamat IP publik. |
| Merujuk objek alamat IP atau objek grup alamat IP dalam templat parameter. | - |

**Protocol port** (Port protokol): masukkan jenis protokol dan rentang port atau rujukan protokol/port atau grup protokol/port dalam templat parameter. Jenis protokol yang didukung termasuk TCP, UDP, ICMP, ICMPv6 dan GRE dalam format berikut.
Port tunggal: seperti `TCP:80`.
Beberapa port: seperti `TCP:80,443`.
Jangkauan port: seperti `TCP:3306-20000`.
Semua port: seperti `TCP:ALL`.
**Policy** (Kebijakan): **Allow** (Izinkan) atau **Refuse** (Tolak). **Allow** (Izinkan) dipilih secara default.
Izinkan: lalu lintas ke port ini diizinkan.

Tolak: paket data akan dibuang tanpa respons apa pun.

**Notes** (Catatan): deskripsi singkat tentang aturan untuk pengelolaan yang lebih mudah.

7.

Klik **Complete** (Selesai) untuk menyelesaikan penambahan aturan.

8. Untuk menambahkan aturan keluar, klik **Outbound rule** (Aturan keluar) dan lihat Langkah 5 ke Langkah 7.

# Mengaitkan Instans CVM dengan Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:47

**Keterangan:**
Grup Keamanan dapat dikaitkan dengan CVM, ENI, database cloud, dan CLB. Dalam dokumen ini, kami menggunakan CVM sebagai contoh.

## Skenario

Grup keamanan dapat dikaitkan dengan satu atau beberapa CVM untuk kontrol akses jaringan. Grup keamanan adalah bagian penting dari langkah-langkah keamanan jaringan CVM. Anda dapat mengaitkan CVM Anda dengan satu atau beberapa grup keamanan jika perlu. Berikut adalah petunjuk selengkapnya.

## Prasyarat

Anda harus sudah membuat instans CVM sebelum memulai.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah yang diinginkan, lalu temukan grup keamanan.
4. Di bawah **Operation** (Operasi), klik **Manage Instances** (Kelola Instans) yang sesuai dengan grup keamanan yang diinginkan. Halaman **Bind with Instance** (Ikat dengan Instans) kemudian akan muncul.
5. Klik **Add Instance** (Tambahkan Instans). Halaman **Add Instance** (Tambahkan Instans) kemudian akan muncul.
6. Pilih instans yang diinginkan, lalu klik **OK** (OKE) untuk menambahkan.

## Lihat Juga

Anda dapat memeriksa semua grup keamanan di wilayah tertentu.
Lihat Melihat Grup Keamanan.

Jika Anda ingin memisahkan instans CVM dengan satu atau beberapa grup keamanan, Anda dapat menghapusnya dari grup keamanan.
Lihat Menghapus Dari Grup Keamanan.
Jika Anda tidak lagi memerlukan grup keamanan, Anda dapat menghapusnya. Setelah grup keamanan dihapus, semua aturan di dalamnya juga dihapus.
Lihat Menghapus Grup Keamanan.

# Mengelola Grup Keamanan

# Melihat Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:48

## Skenario

Artikel ini menjelaskan cara melihat semua grup keamanan suatu wilayah.

## Petunjuk

### Melihat grup keamanan

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah untuk melihat daftar grup keamanan di bawah wilayah tersebut

### Mencari grup keamanan

Anda juga dapat menggunakan bilah pencarian di halaman Grup Keamanan untuk menemukan grup keamanan tertentu dengan cepat.

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pada halaman Pengelolaan Grup Keamanan, pilih **Regions** (Wilayah).
4. Klik bilah pencarian dan gunakan salah satu bidang berikut untuk mencari grup keamanan.

ID Grup Keamanan: masukkan ID yang diinginkan dan klik


untuk melihat grup keamanan yang sesuai.

Nama Grup Keamanan: masukkan nama yang diinginkan dan klik


untuk melihat grup keamanan yang sesuai.

Tag: masukkan tag dan klik


untuk melihat daftar semua grup keamanan dengan tag tersebut.

# Operasi Lainnya

Untuk mempelajari lebih lanjut tentang cara mencari grup keamanan, klik

.

# Hapus dari Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:48

## Skenario

Anda dapat menghapus instans CVM dari grup keamanan jika perlu.

## Prasyarat

Instans dikaitkan dengan dua atau beberapa grup keamanan.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah yang diinginkan dan temukan grup keamanan yang diinginkan.
4. Klik tombol **Manage Instances** (Kelola Instans) yang sesuai untuk membuka halaman **Bind with Instance** (Ikat dengan Instans).
5. Pilih instans yang akan dihapus, lalu klik **Remove Selected** (Hapus yang Dipilih).
6. Di jendela pop-up, klik **OK** (OKE).

# Mengkloning Grup Keamanan

Waktu update terbaru：2022-07-11 16:59:12

## Skenario

Anda mungkin perlu mengkloning grup keamanan jika Anda:
Telah membuat grup keamanan sg-A di wilayah A dan Anda ingin menerapkan aturan yang sama ke instans di wilayah B. Anda dapat mengkloning sg-A ke wilayah B, daripada membuat grup keamanan baru dari awal.
Memerlukan grup keamanan baru untuk layanan Anda tetapi ingin mengkloning grup keamanan lama sebagai cadangan.

## Catatan

Secara default, saat Anda mengkloning grup keamanan, hanya aturan yang dikloning, bukan asosiasi dengan instans. Anda dapat mengkloning grup keamanan di seluruh proyek dan wilayah.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah yang diinginkan. Daftar grup keamanan di bawah wilayah kemudian akan muncul.
4. Temukan grup keamanan yang diinginkan, lalu klik **More** (Lainnya). Kemudian klik **Clone** (Kloning). Halaman **Clone security group** (Kloning grup keamanan) kemudian akan muncul.
5. Pilih **Target region** (Wilayah target) dan **Target project** (Proyek target), lalu masukkan **New name** (Nama baru) untuk grup keamanan baru. Klik **OK** (OKE).

# Menghapus Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:48

## Skenario

Jika Anda tidak lagi memerlukan grup keamanan, Anda dapat menghapusnya. Setelah grup keamanan dihapus, semua aturan di dalamnya juga dihapus.

## Prasyarat

Sebelum menghapus grup keamanan, Anda harus menghapus semua instans CVM terkait. Jika tidak, operasi akan gagal. Untuk detailnya, lihat Menghapus Dari Grup Keamanan.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah yang diinginkan, lalu temukan grup keamanan yang akan dihapus
4. Temukan grup keamanan yang diinginkan, lalu klik **Delete** (Hapus).
5. Di jendela pop-up, klik **OK** (OKE).

# Menyesuaikan Prioritas Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:48

## Ikhtisar

Anda dapat mengikat satu atau beberapa grup keamanan ke CVM. Jika Anda telah mengikat beberapa grup keamanan, grup keamanan ini dijalankan berdasarkan prioritasnya. Anda dapat menyesuaikan prioritas sebagai berikut.

## Prasyarat

Instans dikaitkan dengan dua atau beberapa grup keamanan.

## Petunjuk

1. Login ke konsol CVM.
2. Pada halaman pengelolaan instans, klik ID instans CVM untuk membuka halaman detail.
3. Klik tab **Security Groups** (Grup Keamanan) untuk membuka halaman pengelolaan grup keamanan.
4. Di bagian "Bound Security Group" (Ikat Grup Keamanan) di sebelah kanan, klik **Sort** (Urutkan). Klik ikon

di sebelah kanan untuk menyeret grup keamanan ke atas atau ke bawah untuk menyesuaikan prioritasnya. Grup keamanan di atas memiliki prioritas tertinggi.
5. Setelah menyelesaikan penyesuaian, klik **Save** (Simpan).

# Mengelola Aturan Grup Keamanan
# Melihat Aturan Grup Keamanan

Waktu update terbaru：2021-12-13 19:10:03

## Skenario

Setelah menambahkan aturan grup keamanan, Anda dapat melihat detailnya di konsol.

## Prasyarat

Anda telah membuat grup keamanan dan menambahkan setidaknya satu aturan.
Untuk informasi tentang cara membuat grup keamanan dan aturan grup keamanan, lihat Membuat Grup Keamanan dan Menambahkan Aturan Grup Keamanan.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Di halaman **Security Group** (Grup Keamanan), pilih wilayah, dan temukan grup keamanan yang aturannya ingin Anda lihat.
4. Klik ID atau grup keamanan yang diinginkan untuk membuka halaman detail.
5. Pilih **Inbound rule** (Aturan masuk) atau **Outbound rule** (Aturan keluar) untuk melihat semua aturan grup keamanan masuk atau keluar.

# Memodifikasi Aturan Grup Keamanan

Waktu update terbaru：2021-12-13 19:10:03

## Skenario

Artikel ini menjelaskan cara mengubah aturan grup keamanan. Aturan penting karena mereka melindungi instans CVM Anda dari serangan berbahaya. Misalnya, mereka dapat melindungi port tertentu agar tidak disalahgunakan.

## Prasyarat

Pastikan Anda telah membuat grup keamanan dengan aturan.
Lihat Membuat Grup Keamanan dan Menambahkan Aturan Grup Keamanan.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah yang diinginkan, lalu temukan grup keamanan.
4. Temukan grup keamanan yang diinginkan, lalu klik **Modify Rules** (Modifikasi Aturan). Halaman Aturan Grup Keamanan kemudian akan muncul.
5. Gunakan **Inbound rule** (Aturan masuk) dan **Outbound rule** (Aturan keluar) untuk beralih antara aturan grup keamanan masuk dan keluar.
6. Temukan aturan yang diinginkan dan klik **Edit** (Edit) untuk memodifikasinya.

**Keterangan:**
Anda tidak perlu melakukan boot ulang CVM untuk menerapkan perubahan.

# Hapus kebijakan grup keamanan

Waktu update terbaru：2021-12-13 19:10:03

## Skenario

Jika Anda tidak lagi memerlukan aturan grup keamanan, Anda dapat menghapusnya.

## Prasyarat

Anda telah membuat grup keamanan dan menambahkan setidaknya satu aturan.
Untuk informasi tentang cara membuat grup keamanan dan menambahkan aturan grup keamanan ke dalamnya, lihat Membuat Grup Keamanan dan Menambahkan Aturan Grup Keamanan.
Anda telah mengonfirmasi bahwa instans CVM Anda tidak perlu mengizinkan atau melarang akses Internet atau akses jaringan pribadi.

## Petunjuk

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan). Halaman "Grup Keamanan" kemudian akan muncul.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah) dan temukan grup keamanan yang aturannya ingin Anda hapus.
4. Di kolom tindakan, klik **Modify Rule** (Modifikasi Aturan) untuk membuka halaman aturan grup keamanan.
5. Pilih aturan masuk atau keluar dengan mengklik **Inbound Rules** (Aturan Masuk) atau **Outbound Rules** (Aturan Keluar).
6. Temukan aturan grup keamanan yang akan dihapus, lalu klik **Delete** (Hapus) di kolom tindakan.
7. Di jendela yang muncul, klik **OK** (OKE).

# Mengekspor Aturan Grup Keamanan

Waktu update terbaru：2021-12-13 19:10:03

## Skenario

Anda dapat mengekspor aturan grup keamanan dan menyimpannya secara lokal untuk cadangan.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah untuk menampilkan daftar grup keamanan.
4. Klik nama atau ID grup keamanan yang diinginkan. Halaman detail grup keamanan yang dipilih akan muncul.
5. Pilih aturan masuk atau keluar dengan mengklik **Inbound rules** (Aturan masuk) atau **Outbound rules** (Aturan keluar).
6. Klik

untuk mengekspor aturan grup keamanan ke file dan menyimpannya ke perangkat lokal Anda.

# Mengimpor Aturan Grup Keamanan

Waktu update terbaru：2021-12-13 19:10:03

## Skenario

Aturan grup keamanan dapat diimpor dari file. Anda dapat menggunakan fitur ini untuk memulihkan atau membuat aturan grup keamanan dengan cepat.

## Petunjuk

1. Login ke Konsol CVM.
2. Di bilah sisi kiri, pilih **Security Group** ([Grup Keamanan]). Halaman Grup Keamanan kemudian akan muncul.
3. Pilih wilayah yang diinginkan untuk melihat daftar grup keamanan.
4. Temukan grup keamanan yang diinginkan, lalu klik namanya. Halaman Aturan Grup Keamanan akan muncul.
5. Pilih aturan masuk atau keluar dengan mengklik **Inbound rule** (Aturan masuk) atau **Outbound rule** (Aturan keluar).
6. Klik **Import rules** (Impor aturan). Halaman **Batch import - Inbound/Outbound Rules** (Impor batch - Aturan Masuk/Keluar) akan muncul.
7. Klik **Browse** (Jelajahi) dan pilih file templat aturan. Klik **Import** (Impor).

**Keterangan:**
Jika ada aturan yang ada di grup keamanan, ekspor sebelum mengimpor aturan baru. Aturan yang ada akan ditimpa setelah mengimpor.
Jika tidak ada aturan yang ada di grup keamanan, unduh templat terlebih dahulu. Gunakan templat sebagai awal untuk mengubah aturan sesuai keinginan Anda. Kemudian, impor setelah Anda selesai.

# Kasus Penggunaan Grup Keamanan

Waktu update terbaru：2022-07-08 19:29:10

Grup keamanan dapat mengelola akses ke CVM. Anda dapat mengonfigurasi aturan masuk dan keluar untuk grup keamanan guna menentukan apakah server Anda dapat diakses oleh atau dapat mengakses sumber daya jaringan lainnya.

Aturan masuk dan keluar default untuk grup keamanan adalah sebagai berikut:

**To ensure data security, the inbound rule for a security group is a rejection policy that forbids remote access from external networks.** (Untuk memastikan keamanan data, aturan masuk untuk grup keamanan berupa kebijakan penolakan yang melarang akses jarak jauh dari jaringan eksternal.) Untuk mengaktifkan akses publik ke CVM Anda, Anda perlu membuka port yang sesuai ke Internet dalam aturan masuk.

Aturan keluar untuk grup keamanan menentukan apakah CVM Anda dapat mengakses sumber daya jaringan eksternal. Jika Anda memilih **Open all ports** (Buka semua port) atau **Open ports 22, 80, 443, and 3389 and the ICMP protocol** (Buka port 22, 80, 443, dan 3389 dan protokol ICMP), aturan keluar untuk grup keamanan akan membuka semua port ke Internet. Jika Anda memilih aturan grup keamanan kustom, aturan keluar akan memblokir semua port secara default, dan Anda perlu mengonfigurasi aturan keluar untuk membuka port terkait ke Internet.

## Kasus Penggunaan Umum

Dokumen ini menyediakan beberapa kasus penggunaan umum grup keamanan. Anda dapat langsung menggunakan konfigurasi grup keamanan yang direkomendasikan jika kasus penggunaan memenuhi persyaratan Anda.

### Skenario 1: menghubungkan CVM Linux dari jarak jauh melalui SSH

**Case** (Kasus): Anda telah membuat CVM Linux dan ingin menghubungkannya dari jarak jauh melalui SSH.

**Solution** (Solusi): saat menambahkan aturan grup keamanan, atur **Type** (Jenis) ke **Login Linux CVMs(22)** (Login Linux CVM(22)), masukkan alamat IP proksi WebShell untuk **Source** (Sumber), dan buka port TCP 22 ke Internet untuk mengaktifkan login Linux melalui SSH.

Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang IP) ke Internet sesuai kebutuhan. Tindakan ini memungkinkan Anda mengonfigurasi alamat IP sumber CVM yang dapat dihubungkan dari jarak jauh melalui SSH.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
| --- | --- | --- | --- | --- |
| Masuk | Login Linux | Semua alamat IP: 0.0.0.0/0<br>Alamat IP proksi WebShell: seperti yang dijelaskan dalam Pembaruan Alamat IP Proksi WebShell | TCP:22 | Izinkan |

| | | | | |
|---|---|---|---|---|
| | | Alamat IP yang ditentukan: masukkan alamat IP atau rentang IP yang Anda tentukan | | |

### Skenario 2: menghubungkan dari jarak jauh ke Windows CVM melalui RDP

**Case** (Kasus): Anda telah membuat CVM Windows dan ingin menghubungkannya dari jarak jauh menggunakan Remote Desktop (RDP).

**Solution** (Solusi): saat menambahkan aturan grup keamanan, atur **Type** (Jenis) ke **Login Windows CVMs(3389)** (Login Windows CVM(3389)), masukkan alamat IP proksi WebRDP untuk **Source** (Sumber), dan buka port TCP 3389 ke Internet untuk mengaktifkan login jarak jauh ke Windows.

Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang IP) ke Internet sesuai kebutuhan. Tindakan ini memungkinkan Anda mengonfigurasi alamat IP sumber CVM yang dapat dihubungkan dari jarak jauh melalui RDP.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | Login Windows | Semua alamat IP: 0.0.0.0/0<br>Alamat IP proksi WebRDP:<br>81.69.102.0/24<br>106.55.203.0/24<br>101.33.121.0/24<br>101.32.250.0/24<br>Alamat IP yang ditentukan: masukkan alamat IP atau rentang IP yang Anda tentukan | TCP:3389 | Izinkan |

### Skenario 3: melakukan ping ke CVM di Internet

**Case** (Kasus): Anda telah membuat CVM dan ingin menguji apakah komunikasinya dengan CVM lain normal.

**Solution** (Solusi): uji koneksi dengan menggunakan perintah `ping`. Khususnya, saat menambahkan aturan grup keamanan, atur **Type** (Jenis) ke **Ping** (Ping) dan buka port Internet Control Message Protocol (ICMP) ke Internet untuk memungkinkan CVM lain mengakses CVM ini melalui ICMP.

Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang IP) ke Internet sesuai kebutuhan. Tindakan ini memungkinkan Anda mengonfigurasi alamat IP sumber CVM yang dapat mengakses CVM ini melalui ICMP.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | Ping | Semua alamat IP: 0.0.0.0/0<br>Alamat IP yang ditentukan: masukkan alamat IP atau rentang IP yang Anda tentukan | ICMP | Izinkan |

### Skenario 4: login jarak jauh ke CVM melalui Telnet

**Case** (Kasus): Anda ingin login ke CVM dari jarak jauh dengan menggunakan Telnet.

**Solution** (Solusi): saat menambahkan aturan grup keamanan, konfigurasikan aturan grup keamanan berikut:

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | Kustom | Semua alamat IP: 0.0.0.0/0<br>Alamat IP yang ditentukan: masukkan alamat IP atau rentang IP yang Anda tentukan | TCP: 23 | Izinkan |

### Skenario 5: mengizinkan akses ke layanan web melalui HTTP atau HTTPS

**Case** (Kasus): Anda telah membuat situs web dan ingin mengizinkan akses ke situs web Anda melalui HTTP atau HTTPS.

**Solution** (Solusi): saat menambahkan aturan grup keamanan, konfigurasikan aturan grup keamanan berikut sesuai kebutuhan:

Izinkan semua alamat IP publik untuk mengakses situs web ini

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | HTTP (80) | 0.0.0.0/0 | TCP: 80 | Izinkan |
| Masuk | HTTPS (443) | 0.0.0.0/0 | TCP: 443 | Izinkan |

Izinkan beberapa alamat IP publik untuk mengunjungi situs web ini.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | HTTP (80) | Alamat IP atau rentang IP yang diizinkan untuk mengakses situs web Anda | TCP: 80 | Izinkan |
| Masuk | HTTPS (443) | Alamat IP atau rentang IP yang diizinkan untuk mengakses situs web Anda | TCP: 443 | Izinkan |

### Skenario 6: mengizinkan alamat IP eksternal untuk mengakses port tertentu

**Case** (Kasus): Anda telah men-deploy layanan dan ingin port layanan yang ditentukan (seperti port 1101) dapat diakses secara eksternal.

**Solution** (Solusi): saat menambahkan aturan grup keamanan, atur **Type** (Jenis) ke **Custom** (Kustom) dan buka port TCP 1101 ke Internet untuk mengizinkan akses eksternal ke port layanan yang ditentukan.

Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang IP) ke Internet sesuai kebutuhan. Tindakan ini memungkinkan alamat IP sumber untuk mengakses port layanan yang ditentukan.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | Kustom | Semua alamat IP: 0.0.0.0/0<br>Alamat IP yang ditentukan: masukkan alamat IP atau rentang IP yang Anda tentukan | TCP: 1101 | Izinkan |

### Skenario 7: menolak alamat IP eksternal untuk mengakses port tertentu

**Case** (Kasus): Anda telah men-deploy layanan dan ingin mencegah akses eksternal ke port layanan tertentu (seperti port 1102).

**Solution** (Solusi): saat menambahkan aturan grup keamanan, atur **Type** (Jenis) ke **Custom** (Kustom), konfigurasikan port TCP 1102, dan atur **Policy** (Kebijakan) ke **Reject** (Tolak), sehingga layanan eksternal tidak dapat mengakses port layanan yang ditentukan.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Masuk | Kustom | Semua alamat IP: 0.0.0.0/0<br>Alamat IP yang ditentukan: masukkan alamat IP atau rentang IP yang Anda tentukan | TCP: 1102 | Tolak |

### Skenario 8: mengizinkan CVM mengakses hanya alamat IP eksternal tertentu

**Case** (Kasus): Anda ingin CVM Anda hanya mengakses alamat IP eksternal yang ditentukan.

**Solution** (Solusi): tambahkan dua aturan grup keamanan keluar sebagai berikut.

Izinkan instans CVM mengakses alamat IP eksternal yang ditentukan.

Larang instans CVM mengakses alamat IP publik apa pun melalui protokol apa pun.

**Perhatian:**

Aturan pertama lebih diprioritaskan daripada yang kedua.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| Keluar | Kustom | Alamat IP publik tertentu yang dapat diakses CVM | Protokol dan nomor port yang diperlukan | Izinkan |
| Keluar | Kustom | 0.0.0.0/0 | Semua | Tolak |

### Skenario 9: melarang CVM mengakses alamat IP eksternal tertentu

**Case** (Kasus): Anda tidak ingin CVM Anda mengakses alamat IP eksternal yang ditentukan.

**Solution** (Solusi): tambahkan aturan grup keamanan sebagai berikut.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Keluar | Kustom | Alamat IP publik yang ditentukan yang tidak dapat diakses oleh instans CVM Anda | Semua | Tolak |

### Skenario 10: mengunggah atau mengunduh file dari CVM melalui FTP

**Case** (Kasus): Anda ingin mengizinkan unggahan dan unduhan melalui FTP.

**Solution** (Solusi): tambahkan aturan grup keamanan sebagai berikut.

| Petunjuk | Jenis | Sumber | Port Protokol | Kebijakan |
|---|---|---|---|---|
| TCP | Kustom | 0.0.0.0/0 | Masuk: 20 hingga 21 | Izinkan |

## Konfigurasi Multi-skenario

Anda dapat mengonfigurasi beberapa aturan grup keamanan untuk memenuhi kebutuhan bisnis Anda. Misalnya, aturan masuk dan keluar dapat dikonfigurasi secara bersamaan. Instans CVM dapat diikat ke satu atau beberapa grup keamanan. Ketika terikat ke beberapa grup keamanan, aturan grup keamanan akan dicocokkan secara berurutan dari atas ke bawah. Anda dapat menyesuaikan prioritas grup keamanan kapan saja. Untuk informasi selengkapnya tentang prioritas, lihat Prioritas Aturan.

# Port Umum Server

Waktu update terbaru：2021-12-13 18:24:48

Dokumen ini menjelaskan port server umum. Untuk informasi selengkapnya tentang port aplikasi layanan untuk Windows, lihat Ikhtisar Layanan dan Persyaratan Port Jaringan untuk Windows.

| Port | Layanan | Deskripsi |
| --- | --- | --- |
| 21 | FTP | Port server FTP terbuka untuk mengunggah dan mengunduh. |
| 22 | SSH | Port SSH untuk koneksi jarak jauh ke server Linux dalam mode CLI. |
| 25 | SMTP | Port server SMTP terbuka untuk mengirim email. |
| 80 | HTTP | Port untuk layanan web, seperti IIS, Apache, dan Nginx, untuk menyediakan akses eksternal. |
| 110 | POP3 | Port untuk layanan POP3 (protokol email 3). |
| 137, 138, 139 | Protokol NetBIOS | Port 137 dan 138 adalah port UDP untuk mentransfer file melalui My Network Places. Port 139: koneksi yang dibuat melalui port 139 mencoba mengakses layanan NetBIOS/SMB. Protokol ini digunakan untuk berbagi file dan printer di Windows dan SAMBA. |
| 143 | IMAP | Port untuk Internet Message Access Protocol (IMAP) v2, yang merupakan protokol untuk menerima email seperti POP3. |
| 443 | HTTPS | Port untuk penjelajahan web. HTTPS adalah varian dari HTTP yang menyediakan enkripsi dan transmisi melalui port aman. |
| 1433 | SQL Server | Port default untuk SQL Server. Layanan SQL Server menggunakan dua port: TCP-1433 dan UDP-1434. Port 1433 digunakan untuk menyediakan layanan eksternal, dan port 1434 digunakan untuk menampilkan respons ke pemohon untuk menunjukkan port TCP/IP yang digunakan oleh SQL Server. |
| 3306 | MySQL | Port default untuk database MySQL, yang digunakan oleh MySQL untuk menyediakan layanan eksternal. |
| 3389 | Layanan Desktop Jarak Jauh Windows Server | Port layanan untuk desktop jarak jauh Windows Server, tempat Anda dapat menyambung ke server jauh menggunakan alat sambungan "Desktop Jarak Jauh". |
| 8080 | Port | Mirip dengan port 80, port 8080 digunakan dalam layanan proksi WWW untuk |

| | | |
|---|---|---|
| | proksi | penjelajahan web. Nomor port ":8080" sering ditambahkan ke URL saat Anda mengunjungi situs web atau menggunakan proksi. Selain itu, setelah server web Apache Tomcat diinstal, port layanan default-nya adalah port 8080. |

# Ikhtisar API Grup Keamanan

Waktu update terbaru：2021-12-13 18:24:49

| Nama API | Deskripsi |
| --- | --- |
| CreateSecurityGroup | Buat grup keamanan |
| CreateSecurityGroupPolicies | Buat aturan grup keamanan |
| DeleteSecurityGroup | Hapus grup keamanan |
| DeleteSecurityGroupPolicies | Hapus aturan grup keamanan |
| DescribeSecurityGroupAssociationStatistics | Buat kueri statistik instans yang terkait dengan grup keamanan |
| DescribeSecurityGroupPolicies | Buat kueri aturan grup keamanan |
| DescribeSecurityGroups | Buat kueri grup keamanan |
| ModifySecurityGroupAttribute | Ubah atribut grup keamanan |
| ModifySecurityGroupPolicies | Ubah aturan masuk dan keluar grup keamanan |
| ReplaceSecurityGroupPolicy | Ganti satu aturan grup keamanan |

# Perlindungan Operasi Sensitif

Waktu update terbaru：2021-12-13 18:24:49

## Ikhtisar

Fitur perlindungan operasi sensitif saat ini tersedia di CVM. Setelah fitur diaktifkan, selesaikan verifikasi identitas sebelum melakukan operasi sensitif.
Fitur ini dapat secara efektif melindungi keamanan sumber daya akun, termasuk penonaktifan, mulai ulang, login VNC, atur ulang kata sandi, penghentian instans, penginstalan ulang sistem, penyesuaian konfigurasi, pemuatan kunci, dan beralih VPC.

## Mengaktifkan Perlindungan Operasi

Anda dapat mengaktifkan fitur perlindungan operasi di konsol Pengaturan Keamanan. Untuk informasi selengkapnya, lihat Perlindungan Operasi.

## Memverifikasi Perlindungan Operasi

Setelah perlindungan operasi diaktifkan, Anda harus menyelesaikan verifikasi identitas sebelum dapat melakukan operasi sensitif:
Jika Anda telah mengaktifkan **MFA verification** (Verifikasi MFA) untuk perlindungan operasi, Anda harus memasukkan kode verifikasi dinamis 6 digit yang ditampilkan pada perangkat MFA.
Jika Anda telah mengaktifkan **SMS code verification** (Verifikasi kode SMS) untuk perlindungan operasi, Anda harus memasukkan kode verifikasi yang diterima di ponsel Anda.

# Mengelola Kata Sandi Login

Waktu update terbaru：2022-09-20 15:17:23

## Pengantar

Akun dan kata sandi CVM dapat digunakan sebagai kredensial untuk instans CVM. Artikel ini menjelaskan cara menggunakan dan mengelola kata sandi saat login ke instans CVM.

## Persyaratan Kata Sandi

Kata sandi harus memenuhi persyaratan ini:
Kata sandi instans Linux: kata sandi harus terdiri dari 8 hingga 30 karakter. Sebaiknya gunakan kata sandi minimal 12 karakter. Kata sandi tidak boleh dimulai dengan `/` dan harus berisi setidaknya tiga hal berikut: ( `a-z` , `A-Z` , `0-9` , dan simbol khusus `()` `~!@#$%^&*-+=_|{}[]:;'<>,.?/` ).
Kata sandi instans Windows: kata sandi harus terdiri dari 12 hingga 30 karakter. Kata sandi tidak boleh dimulai dengan `/` dan harus berisi setidaknya tiga hal berikut: ( `a-z` , `A-Z` , `0-9` , dan simbol khusus `()` `~!@#$%^&*-+=_|{}[]:;'<>,.?/` ), dan tidak boleh berisi nama pengguna Anda.

## Petunjuk

### Mengatur kata sandi awal

Ada dua cara untuk mengatur kata sandi awal, bergantung pada cara Anda mengonfigurasi instans CVM saat membelinya:
Jika Anda menggunakan opsi **Konfigurasi Cepat**, kata sandi awal dikirimkan kepada Anda melalui email dan pesan ke konsol Pusat Pesan.
Jika Anda menggunakan opsi **Konfigurasi Kustom**, kata sandi awal diatur dengan cara berikut tergantung pada cara Anda memilih untuk login:

| Metode Login | Deskripsi |
| --- | --- |
| Pembuatan kata sandi otomatis | Kata sandi awal dikirimkan kepada Anda melalui email dan konsol Pusat Pesan. |
| Kaitkan kunci sekarang | **Dinonaktifkan secara default**. Anda login menggunakan nama pengguna dan kata sandi, namun kata sandi awal dikirimkan kepada Anda melalui email dan Pusat Pesan konsol. |

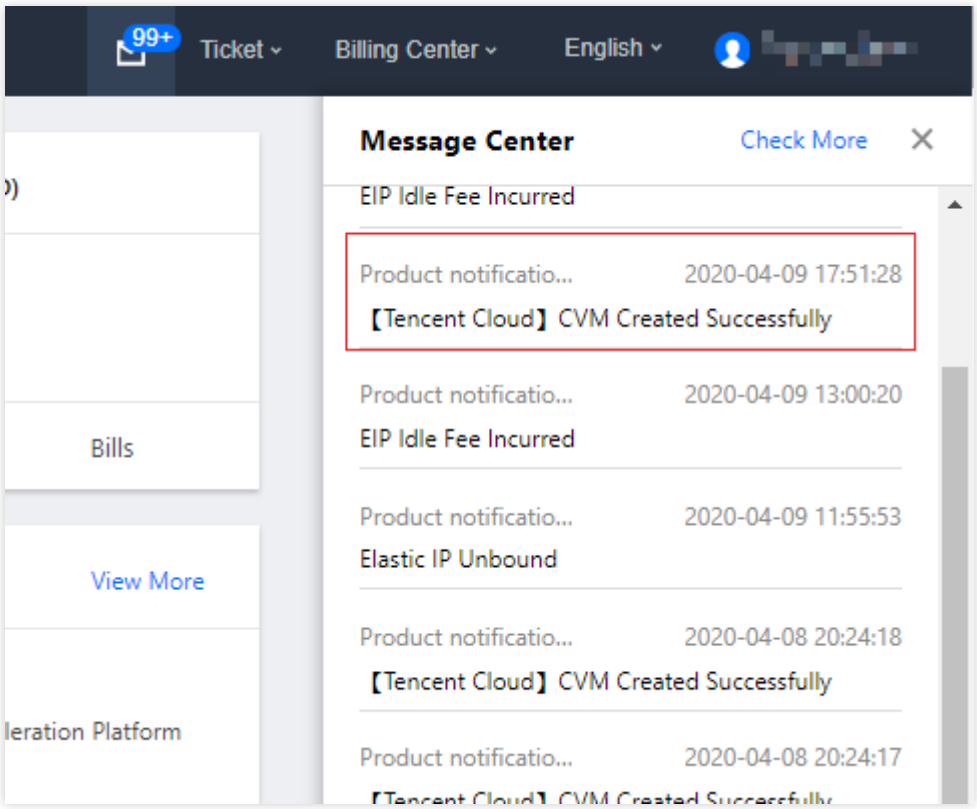
| | |
|---|---|
| Atur kata sandi | Anda mengatur kata sandi awal. |

## Melihat kata sandi

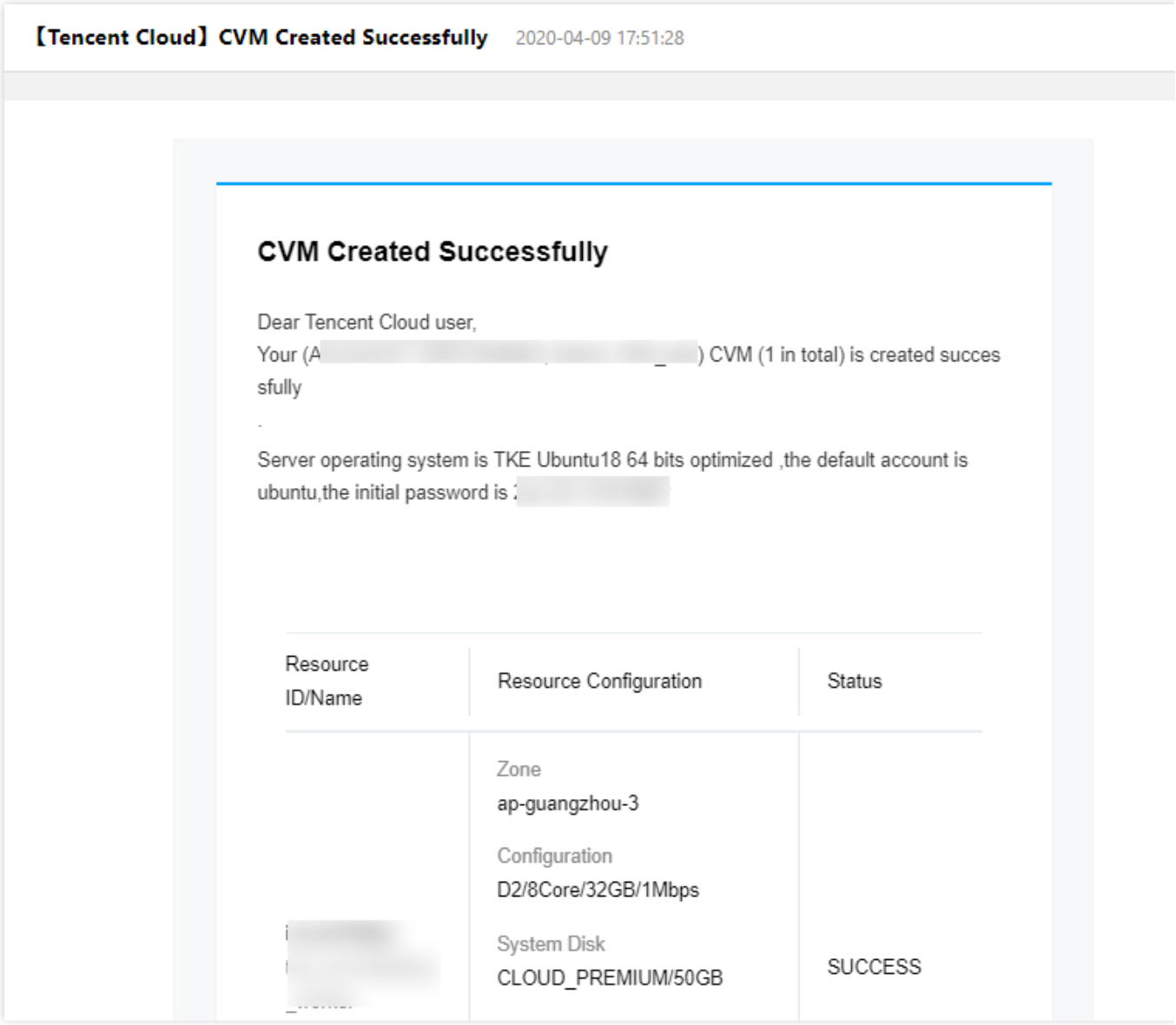
Kata sandi login Anda dikirimkan kepada Anda melalui email dan konsol Pusat Pesan. Berikut ini menjelaskan cara memeriksa pesan Anda di pusat pesan.

1. Login ke Konsol CVM.
2. Klik

di sudut kanan atas dan pilih pesan produk yang sesuai, seperti yang ditunjukkan pada gambar berikut:




Lihat kata sandi Anda di halaman pesan.




## Mengatur ulang kata sandi

Untuk petunjuk tentang cara mengatur ulang kata sandi Anda, lihat Mengatur Ulang Kata Sandi Instans.

# Mengelola kunci SSH

Waktu update terbaru：2022-01-11 16:23:42

## Ikhtisar

Dokumen ini menjelaskan operasi umum yang terkait dengan penggunaan pasangan kunci SSH untuk masuk ke instans. Misalnya, Anda dapat membuat, mengikat, melepas ikatan, memodifikasi, atau menghapus pasangan kunci SSH.

**Perhatian:**

Untuk mengikat kunci SSH ke atau melepas ikatan dari sebuah instans, harap matikan instans terlebih dahulu. Lihat Mematikan Instans.

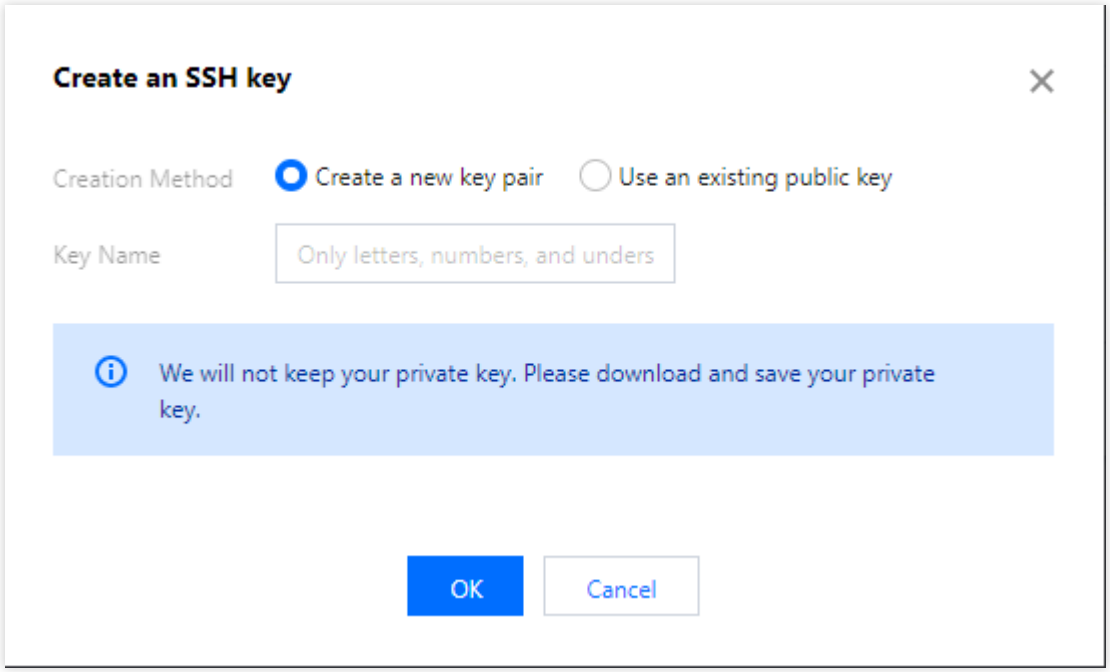
## Petunjuk

### Membuat kunci SSH

1. Login ke konsol CVM.
2. Klik **SSh Key** (Kunci SSH) di bilah sisi kiri.
3. Klik **New** (Baru) di halaman **SSH key** (Kunci SSH).

**Perhatian:**

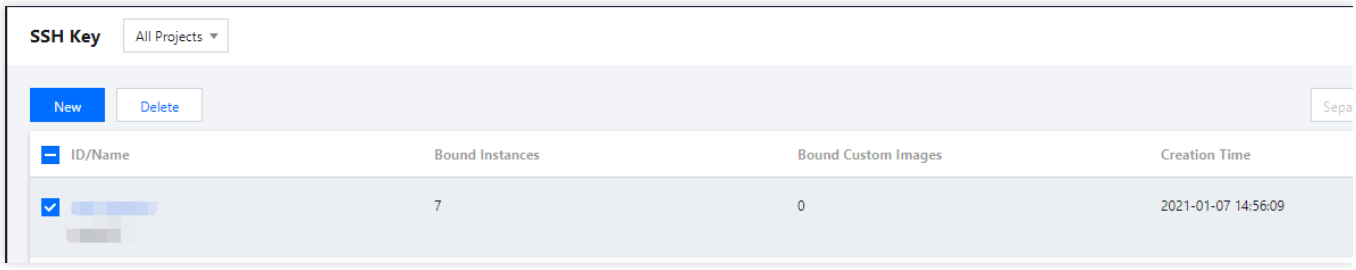
Setelah mengklik **OK** (OKE), kunci pribadi akan diunduh secara otomatis. Tencent Cloud tidak akan menyimpan kunci pribadi Anda. Pastikan untuk menyimpannya dengan aman.




Jika Anda memilih **Create a new key pair** (Buat pasangan kunci baru), masukkan nama kunci.
Jika Anda memilih **Use an existing public key** (Gunakan kunci publik yang ada), masukkan nama kunci dan informasi kunci publik asli.

## Mengikat kunci ke instans

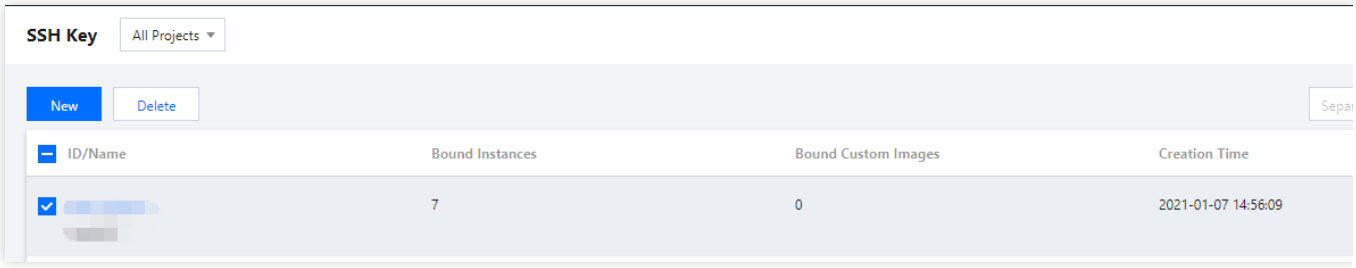
1. Login ke konsol CVM.
2. Klik **SSh Key** (Kunci SSH) di bilah sisi kiri.
3. Pada halaman pengelolaan kunci SSH, pilih kunci SSH target, lalu klik **Bind with instances** (Ikat dengan instans).




4. Di jendela pop-up, pilih wilayah target dan instans, lalu klik **Bind** (Ikat).

## Melepas kunci dari instans

1. Login ke konsol CVM.
2. Klik **SSh Key** (Kunci SSH) di bilah sisi kiri.
3. Pada halaman pengelolaan kunci SSH, pilih kunci SSH target, lalu klik **Unbind from instances** (Lepaskan dari instans).

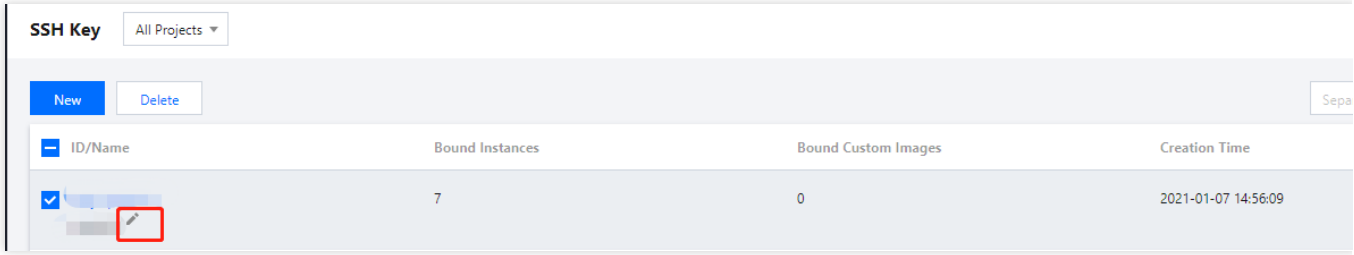



4. Di jendela pop-up, pilih wilayah dan instans yang akan dilepas dari kunci, lalu klik **Unbind** (Lepaskan ikatan).

## Memodifikasi nama atau deskripsi kunci SSH

1. Login ke konsol CVM.
2. Klik **SSh Key** (Kunci SSH) di bilah sisi kiri.
3. Pada halaman pengelolaan kunci SSH, pilih kunci yang akan dimodifikasi dan klik

di sebelah nama kunci, seperti yang ditunjukkan di bawah ini.




4. Di jendela pop-up, masukkan nama atau deskripsi kunci baru, dan klik **OK** (OKE).

## Menghapus kunci SSH

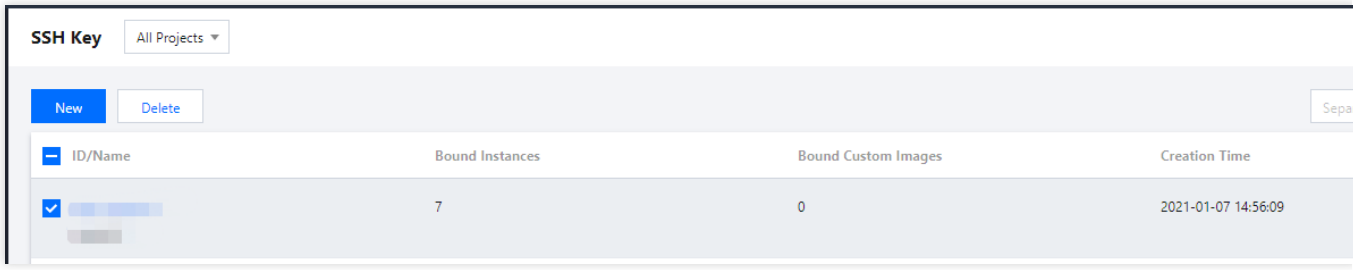
**Perhatian:**

Kunci SSH tidak dapat dihapus ketika terikat dengan instans CVM atau citra kustom, tidak dapat dihapus.

1. Login ke konsol CVM.
2. Klik **SSh Key** (Kunci SSH) di bilah sisi kiri. Anda dapat menghapus satu atau beberapa kunci SSH sesuai kebutuhan.

**Deleting a single key** (Menghapus satu kunci)

2.1.1 Pada halaman pengelolaan kunci SSH, pilih kunci SSH yang akan dihapus, lalu klik **Delete** (Hapus) di bawah kolom **Operation** (Operasi), seperti yang ditunjukkan di bawah ini.



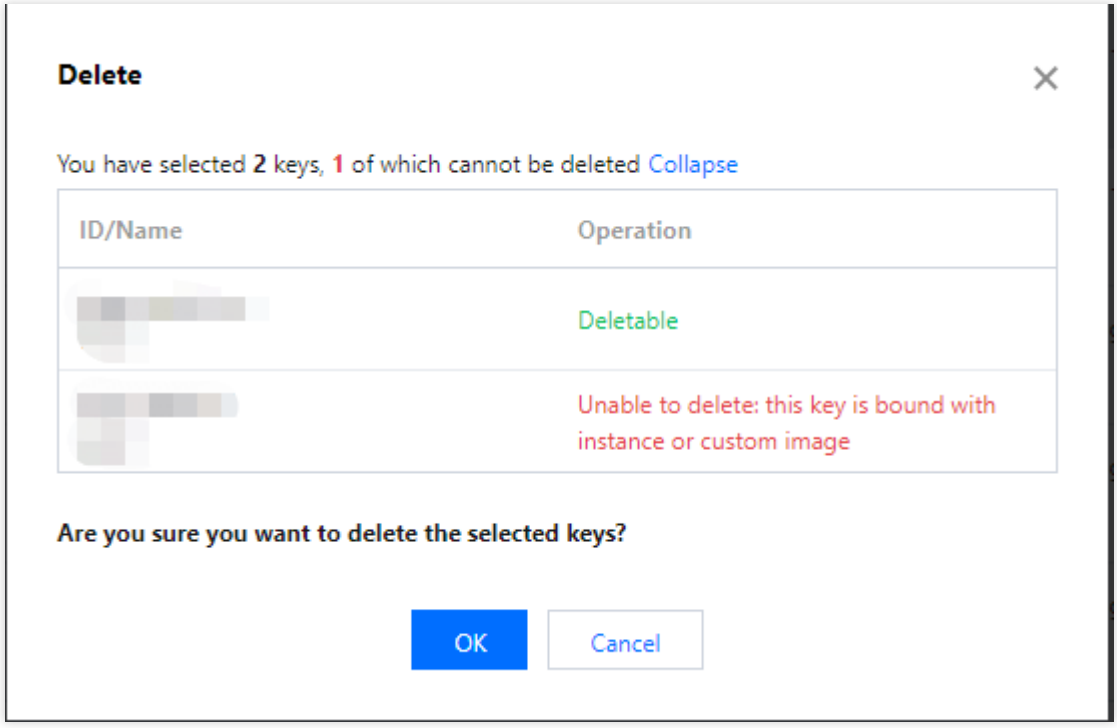

2.1.2 Di jendela pop-up, klik **OK** (OKE).

**Batch deleting keys** (Kunci penghapusan batch)

2.1.1 Pada halaman pengelolaan kunci SSH, pilih kunci SSH yang akan dihapus, lalu klik **Delete** (Hapus) di atas daftar untuk menghapusnya per batch.

2.1.2 Di jendela pop-up, klik **OK** (OKE), seperti yang ditunjukkan di bawah ini.

Hanya kunci yang dapat dihapus dari pasangan kunci yang dipilih yang akan dihapus.




## Menggunakan kunci SSH untuk login ke CVM Linux

1. Buat kunci SSH.
2. Ikat kunci SSH ke instans CVM.
3. Masuk ke instans Linux melalui kunci SSH.

# Grup Penempatan Tersebar

Waktu update terbaru：2021-12-13 18:24:49

## Skenario

Dokumen ini menjelaskan cara mengelola grup penempatan sebaran. Untuk informasi selengkapnya tentang grup penempatan, lihat Grup Penempatan.

## Petunjuk

### Membuat grup penempatan

1. Login ke konsol grup penempatan CVM.
2. Klik **Create** (Buat).
3. Di jendela yang muncul, masukkan nama untuk grup penempatan, dan pilih lapisan grup penempatan.
4. Klik **OK** (OKE) untuk menyelesaikan pembuatan.

### Memulai instans di grup penempatan

1. Buka halaman pembelian CVM.
2. Selesaikan pembelian seperti yang diminta di halaman.

Selama proses pembelian, pastikan untuk melakukan operasi berikut:

Saat mengatur CVM, klik **Advanced Configuration** (Konfigurasi Lanjutan), pilih **Add Instance to Placement Group** (Tambahkan Instans ke Grup Penempatan), dan pilih grup penempatan yang sudah ada.

Jika tidak ada grup penempatan yang memenuhi persyaratan Anda, buat satu di konsol.

Saat mengonfirmasi informasi konfigurasi, masukkan jumlah total instans yang akan ditambahkan ke grup penempatan, yang harus kurang dari batas kuantitas yang ditetapkan untuk grup penempatan.

### Memodifikasi grup penempatan instans

**Keterangan:**

Saat ini, Anda hanya dapat mengubah nama grup penempatan. Untuk melakukannya, selesaikan langkah-langkah berikut.

1. Login ke konsol grup penempatan CVM.
2. Arahkan kursor ke ID atau nama grup penempatan target, lalu klik

.

3. Di jendela yang muncul, masukkan nama baru.
4. Klik **OK** (OKE) untuk menyelesaikan modifikasi.

## Menghapus grup penempatan

**Keterangan:**

Anda dapat menghapus grup penempatan yang perlu diganti atau tidak lagi diperlukan. Anda harus menghentikan semua instans yang berjalan di grup penempatan sebelum dapat menghapusnya. Untuk melakukannya, selesaikan langkah-langkah berikut.

1. Login ke konsol grup penempatan CVM.
2. Klik **Number of Instances** (Jumlah Instans) untuk grup penempatan yang akan dihapus untuk membuka halaman pengelolaan instans, dan menghentikan semua instans dalam grup penempatan.
3. Kembali ke konsol grup penempatan, pilih grup penempatan yang akan dihapus, lalu klik **Delete** (Hapus).
4. Di jendela yang muncul, klik **OK** (OKE) untuk menyelesaikan penghapusan.

Anda dapat menghapus satu grup penempatan atau beberapa grup penempatan secara massal.

# Membuka Blokir Port 25

Waktu update terbaru：2021-12-13 18:24:49

## Pengantar

Artikel ini menjelaskan cara membuka pemblokiran port 25.

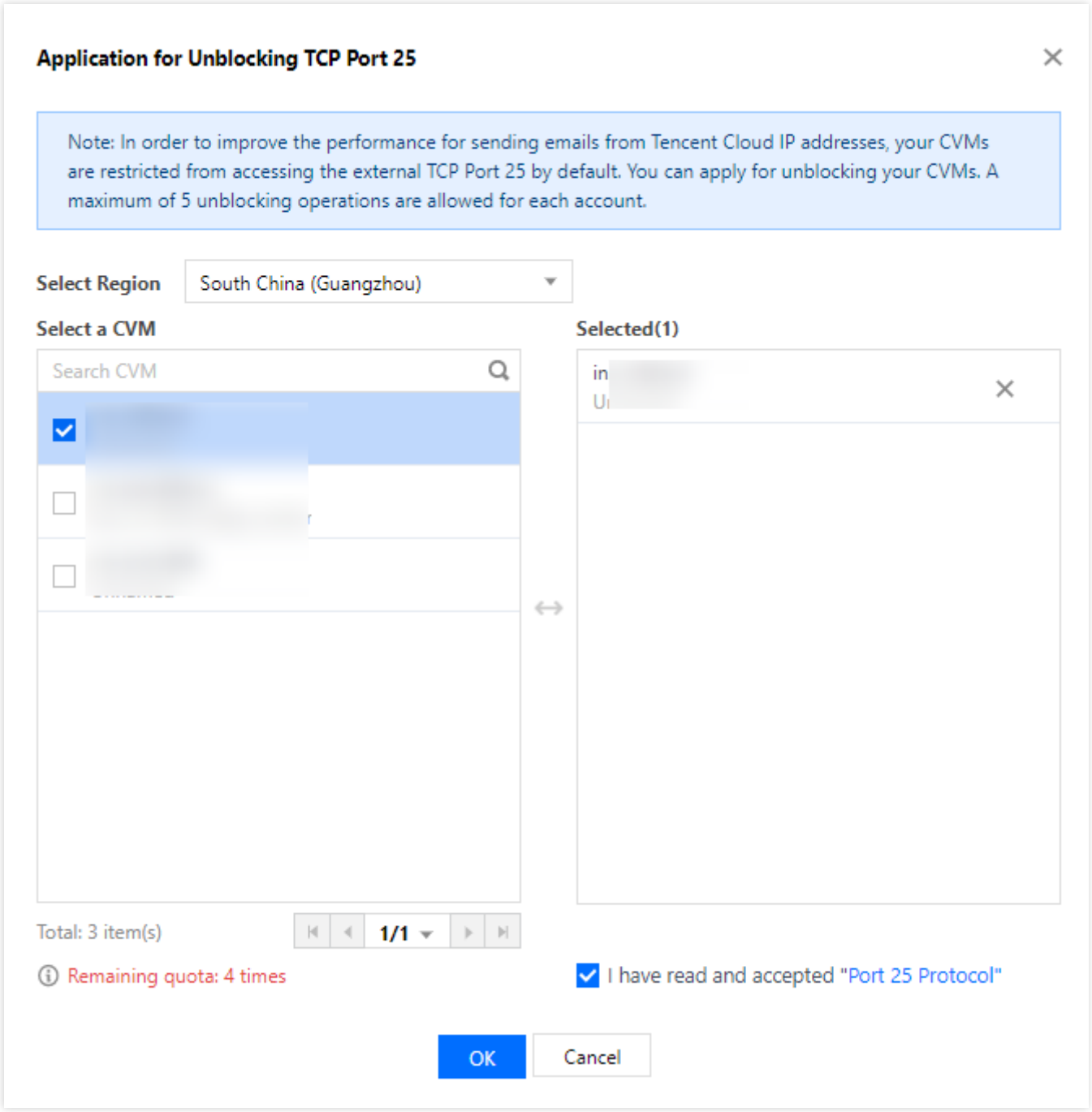
## Catatan

Anda hanya dapat membuka pemblokiran port 25 bagi lima instans untuk setiap akun Tencent Cloud.
Pastikan Anda hanya menggunakan port 25 untuk terhubung ke server SMTP pihak ketiga untuk mengirim email.
Jika Anda menggunakan CVM Anda untuk mengirim email secara langsung, kami berhak melarang Anda membuka port 25 secara permanen.

## Petunjuk

1. Login ke Konsol Tencent Cloud.
2. Klik nama akun Anda di sudut kanan atas. Pilih **Security Management** ([Pengelolaan Keamanan]).
3. Di bilah sisi kiri, klik **Unblock port 25** (Buka pemblokiran port 25) untuk membuka halaman **Unblock port 25** (Buka pemblokiran port 25).
4. Klik **Apply for unblocking port 25** (Terapkan untuk membuka pemblokiran port 25) untuk membuka jendela **Apply for unblocking port 25** (Terapkan untuk membuka pemblokiran port 25).
5. Pilih wilayah dan instans CVM yang perlu dibuka pemblokirannya. Pilih **I have read and agree to the port 25 usage agreement.** (Saya telah membaca dan menyetujui perjanjian penggunaan port 25.), seperti yang ditunjukkan di bawah ini:

**Keterangan:**
Pastikan Anda belum menghabiskan kuota buka pemblokiran Anda. Anda dapat memeriksa sisa kuota di kiri bawah pada jendela **Apply for unblocking port 25** (Terapkan untuk membuka pemblokiran port 25).




6. Klik **OK** (OKE) untuk menyelesaikan proses.

# Tag
# Mengelola Instans melalui Tag

Waktu update terbaru：2021-12-13 19:10:04

## Ikhtisar

**Tag** (Tag) adalah pasangan nilai kunci yang disediakan oleh Tencent Cloud untuk memudahkan identifikasi sumber daya. Anda dapat menggunakan tag untuk mengategorikan dan mengelola sumber daya CVM Anda.
Tencent Cloud tidak akan menggunakan tag Anda, tag tersebut hanya digunakan oleh Anda untuk mengelola sumber daya CVM Anda.

## Batasan Penggunaan

Perhatikan batasan berikut saat menggunakan tag:
Batas kuantitas: setiap sumber daya Tencent Cloud memungkinkan hingga 50 tag.
Batas kunci tag:
Kunci tag tidak dapat dimulai dengan `qcloud` , `tencent` , atau `project` .
Kunci tag dapat berisi hingga 255 karakter, termasuk angka, huruf, dan `+=.@-` .
Batas nilai tag: nilai tag dapat berisi hingga 127 karakter, termasuk angka, huruf, dan `+=.@-` . Nilai ini bisa dibiarkan kosong jika perlu.

## Petunjuk dan Kasus

### Kasus penggunaan

Sebuah perusahaan telah membeli enam instans CVM, dengan grup bisnis, cakupan, dan pemiliknya adalah sebagai berikut:

| ID Instans | Grup Bisnis | Cakupan Bisnis | Pemilik |
|---|---|---|---|
| ins-abcdef1 | E-commerce | Kampanye pemasaran | John Smith |
| ins-abcdef2 | E-commerce | Kampanye pemasaran | Chris |
| ins-abcdef3 | Game | Game A | Jane Smith |
| ins-abcdef4 | Game | Game B | Chris |

| | | | |
|---|---|---|---|
| ins-abcdef5 | Hiburan | Pasca produksi | Chris |
| ins-abcdef6 | Hiburan | Pasca produksi | John Smith |

Mengambil ins-abcdef1 sebagai contoh, kami dapat menambahkan 3 set tag berikut ke instans:

| Tag Key | Tag Value |
|---|---|
| dept | ecommerce |
| business | mkt |
| owner | John Smith |

Demikian pula, Anda dapat menambahkan pasangan nilai kunci tag ke instans lain berdasarkan grup bisnis, cakupan, dan pemilik.

### Mengatur tag di konsol CVM

Ambil kasus sebelumnya sebagai contoh. Setelah mendesain pasangan nilai kunci tag, Anda dapat masuk ke konsol CVM untuk menentukan tag.

1. Login ke konsol CVM.
2. Pada halaman **Instance** (Instans), pilih instans target dan klik **More** (Lainnya) > **Instance Settings** (Pengaturan Instans) > **Edit Tags** (Edit Tag) di kolom **Operation** (Operasi).
3. Atur tag di bagian "1 sumber daya yang dipilih" dari jendela pop-up.
Misalnya, Anda dapat menambahkan tiga pasangan nilai kunci tag ke instans ins-abcdef1.
4. Klik **OK** (OKE). Sistem menampilkan pesan yang menunjukkan bahwa modifikasi berhasil.

### Memfilter instans berdasarkan tag

Untuk memfilter instans menurut tag, ikuti langkah-langkah di bawah ini:

1. Klik kotak pencarian dan pilih **Tag** (Tag) dari daftar drop-down.
2. Masukkan tag, dan klik


untuk menelusuri.

Anda dapat memfilter instans menggunakan tag. Misalnya, Anda dapat mencari instans yang terikat dengan tag `key1` atau `key2` dengan memasukkan `Tag: key1|key2` di kotak pencarian.

# Edit Tag

Waktu update terbaru：2021-12-13 19:10:04

## Skenario Operasi

Dokumen ini menjelaskan cara mengedit tag sumber daya.

## Batasan Penggunaan

Ada beberapa batasan dalam mengedit tag:
Kuantitas: setiap sumber daya dapat memiliki paling banyak 50 tag.
Pembatasan kunci tag:
Anda tidak dapat membuat kunci tag yang dimulai dengan `qcloud` , `tencent` , dan `project` karena dicadangkan untuk sistem.
Kunci tag hanya boleh berisi `angka` , `karakter alfabet` , `+=.@-` , dan harus kurang dari 255 karakter.
Nilai tag: nilai tag hanya boleh berisi `string atau angka kosong` , `karakter alfabet` , `+=.@-` , dan harus kurang dari 127 karakter.

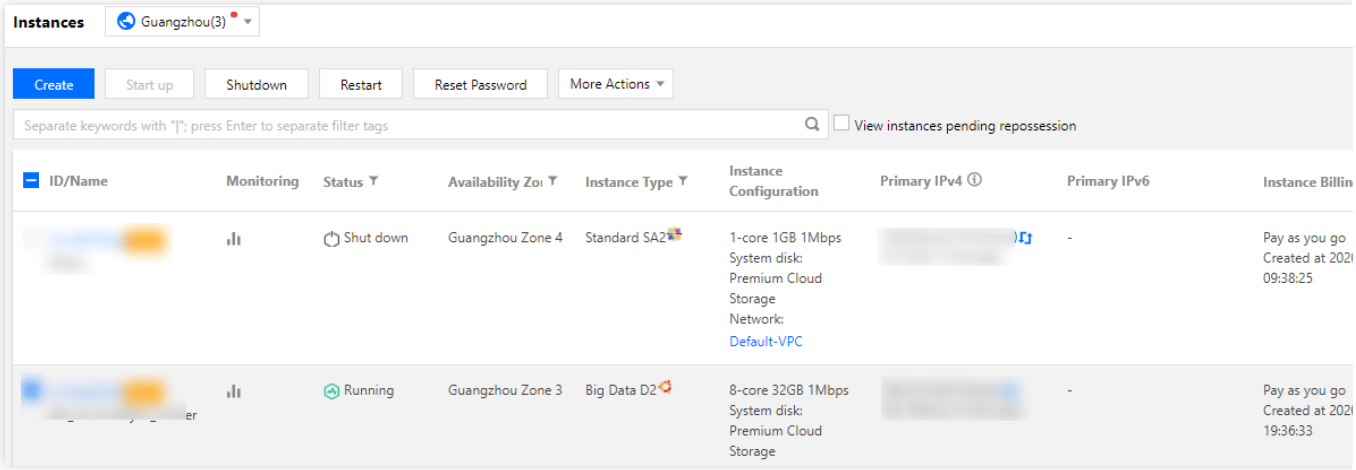
## Prasyarat

Login ke Konsol CVM.

## Petunjuk

### Mengedit tag dari satu instans

1. Pada halaman pengelolaan Instans, pilih instans yang tagnya perlu diedit dan klik **More** (Lainnya) > **Instance Settings** (Pengaturan Instans) > **Edit Tags** (Edit Tag), seperti yang ditunjukkan di bawah ini.



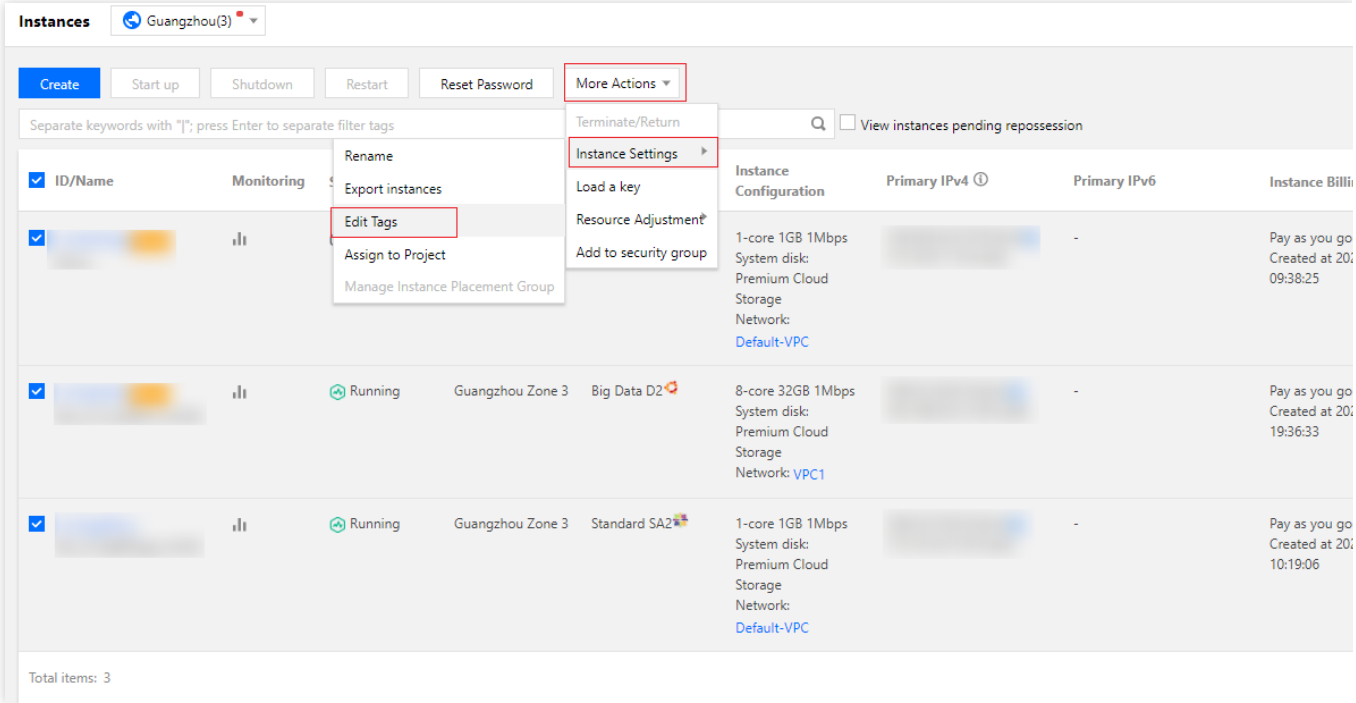

2. Tambahkan, modifikasi, atau hapus tag di jendela pop-up “1 sumber daya cloud yang dipilih” berdasarkan kebutuhan Anda.

## Mengedit tag beberapa instans

**Keterangan:**

Anda dapat mengedit tag hingga 20 sumber sekaligus.

1. Pada halaman pengelolaan Instans, pilih instans yang tagnya perlu diedit dan klik **More Actions** (Tindakan Lainnya) > **Instance Settings** (Pengaturan Instans) > **Edit Tags** (Edit Tag) di bagian atas, seperti yang ditunjukkan di bawah ini:




2. Tambahkan, modifikasi, dan hapus tag di jendela pop-up “n sumber daya cloud yang dipilih” berdasarkan kebutuhan Anda.

# Contoh Operasi

Untuk informasi tentang cara menggunakan tag, harap lihat Panduan Pengguna tentang Tag.

# Pemantauan dan Alarm
# Mendapatkan Statistik Pemantauan

Waktu update terbaru：2022-07-12 16:29:01

## Ikhtisar

Tencent Cloud menyediakan fitur Cloud Monitor untuk semua pengguna secara default. Fitur ini membantu memantau dan mengumpulkan data dari produk Tencent Cloud yang Anda gunakan. Dokumen ini menjelaskan cara mendapatkan data pemantauan.

## Petunjuk

Memperoleh data pemantauan dari konsol CVM
Memperoleh data pemantauan dari konsol Cloud Monitor
Memperoleh data pemantauan dari dasbor Cloud Monitor
Memperoleh data pemantauan melalui API

**Keterangan:**

Konsol CVM menyediakan halaman pemantauan, tempat Anda dapat melihat data pemantauan CPU, memori, bandwidth jaringan, dan disk dalam periode yang ditentukan.

1. Login ke konsol CVM.
2. Di halaman pengelolaan instans, klik ID/Nama CVM untuk masuk ke halaman detailnya dan melihat data pemantauan.
3. Klik tab **Monitoring** (Pemantauan) untuk mendapatkan data pemantauan instans.

**Keterangan:**

Konsol Cloud Monitor menyediakan data pemantauan semua produk Tencent Cloud. Di konsol, Anda dapat melihat data pemantauan CPU, memori, bandwidth jaringan, dan disk dalam periode yang ditentukan.

1. Login ke Konsol Monitor Cloud.
2. Pilih **Cloud Product Monitoring** (Cloud Product Monitoring) > **Cloud Virtual Machine** (Cloud Virtual Machine) di bilah sisi kiri.
3. Klik ID/Nama instans CVM untuk masuk ke halaman detailnya dan melihat data pemantauan.

Tentukan metrik CVM yang diperlukan dan buat dasbor, tempat Anda dapat melihat data pemantauan dalam bagan intuitif, yang membantu Anda menganalisis metrik melalui tren dan nilai luar biasa.

1. Login ke konsol Cloud Monitor, lalu pilih **dashboard** (dasbor) > Default Dashboard(Dasbor Default).
2. Buat dasbor seperti yang diinstruksikan di Buat Dasbor dan dapatkan data pemantauan.

Anda dapat menggunakan `GetMonitorData` API untuk mendapatkan data pemantauan untuk semua produk Tencent Cloud. Untuk informasi selengkapnya, lihat GetMonitorData.

# Buat Kebijakan Alarm

Waktu update terbaru：2022-05-10 11:55:13

## Ikhtisar

Anda dapat mengatur alarm ambang batas untuk memantau performa CVM, serta alarm peristiwa untuk melihat status instans CVM dan infrastruktur platform yang mendasarinya. Ketika terjadi pengecualian, Anda akan segera menerima notifikasi melalui , email, SMS, telepon, dll. Kebijakan alarm yang tepat akan membantu meningkatkan ketahanan dan keandalan aplikasi Anda. Dokumen ini menjelaskan cara membuat kebijakan alarm. Untuk informasi selengkapnya, lihat Membuat Kebijakan Alarm.

## Petunjuk

1. Login ke [Konsol Cloud Monitor], lalu pilih **Alarm Configuration** (Konfigurasi Alarm) > **Alarm Policy** (Kebijakan Alarm) di bilah sisi kiri.
2. Di halaman **Alarm Policy** (Kebijakan Alarm), klik **Create** (Buat).
3. Di jendela pop-up, konfigurasikan informasi dasar, kebijakan alarm, dan templat notifikasi seperti yang diinstruksikan di bawah ini.

| Jenis Konfigurasi | Item Konfigurasi | Deskripsi |
|---|---|---|
| Info Dasar | Nama Kebijakan | Nama kebijakan kustom |
| | Keterangan | Keterangan untuk kebijakan |
| | Jenis Pemantauan | Pilih **Cloud Product Monitoring** |
| | Jenis Kebijakan | Pilih jenis kebijakan yang diinginkan untuk memantau layanan Tencent Cloud. |
| | Proyek | Pilih proyek sesuai kebutuhan. Anda nanti dapat menemukan kebijakan ini dengan cepat dengan memfilter berdasarkan proyek. |
| Konfigurasikan Kebijakan Alarm | Objek Alarm | **ID Instans:** mengaitkan kebijakan dengan instans CVM yang ditentukan<br>**Tag**: mengaitkan kebijakan dengan instans CVM dengan tag yang ditentukan |

| | | | |
|---|---|---|---|
| | | | **Grup Instans**: mengaitkan kebijakan dengan grup instans yang dipilih<br>**Semua Objek**: mengaitkan kebijakan dengan semua instans akun saat ini (diperlukan izin) |
| | Kondisi Pemicu | **Konfigurasi Manual**(Alarm Metrik) | Kondisi pemicu: tentukan metrik, perbandingan, ambang batas, periode statistik, dan jumlah periode berturut-turut. Anda dapat memperluas kondisi pemicu untuk melihat tren metrik, dan berdasarkan pemicu yang menetapkan ambang batas yang tepat. |
| | | **Konfigurasi Manual**(Alarm Peristiwa) | Buat kebijakan alarm peristiwa untuk mendapatkan notifikasi jika ada sumber daya layanan atau pengecualian infrastruktur yang mendasarinya |
| | | Pilih templat | Pilih templat yang dikonfigurasi sesuai kebutuhan. Untuk informasi selengkapnya tentang konfigurasi, harap lihat Mengonfigurasi Templat Kondisi Pemicu. |
| Konfigurasikan Notifikasi Alarm (opsional) | Templat Notifikasi | | Pengaturan default-nya diatur ke templat notifikasi prasetel (mengirim notifikasi ke admin akun root melalui SMS dan email). Setiap kebijakan alarm dapat mengikat hingga 3 templat notifikasi. Untuk informasi selengkapnya tentang konfigurasi templat notifikasi, lihat Membuat Templat Notifikasi. |

4. Klik **Complete** (Selesai).

# Contoh Konsol

Waktu update terbaru：2021-12-13 17:07:08

## Pengantar

Anda dapat menggunakan kebijakan Cloud Access Management (CAM) untuk mengelola akses pengguna ke sumber daya menggunakan konsol Cloud Virtual Machine (CVM). Dokumen ini menyediakan contoh untuk membantu Anda memahami cara menggunakan kebijakan CAM yang telah ditentukan sebelumnya menggunakan konsol CVM.

## Contoh

### Pembacaan dan penulisan (CVM)

Jika Anda ingin mengizinkan pengguna membuat dan mengelola instans CVM, kaitkan pengguna dengan kebijakan bernama QcloudCVMFullAccess. Kebijakan ini dirancang untuk memberikan izin kepada pengguna untuk mengakses semua sumber daya di CVM, Virtual Private Cloud (VPC), Cloud Load Balancer (CLB), dan Cloud Monitor.
Langkah-langkah detailnya adalah sebagai berikut:
Lihat Pengelolaan Otorisasi untuk petunjuk tentang cara memberikan kebijakan prasetel QcloudCVMFullAccess kepada pengguna.

### Hanya baca (CVM)

Jika Anda ingin mengizinkan pengguna untuk hanya membuat kueri, tetapi tidak membuat, menghapus, atau memulai/mematikan instans CVM, kaitkan pengguna dengan kebijakan bernama QcloudCVMInnerReadOnlyAccess. Kebijakan ini dirancang untuk memberikan izin kepada pengguna untuk melakukan semua operasi yang dimulai dengan "Describe" (Jelaskan) dan "Inquiry" (Pertanyaan) di CVM. Langkah-langkah detailnya adalah sebagai berikut:
Lihat Pengelolaan Otorisasi untuk petunjuk tentang cara memberikan kebijakan prasetel QcloudCVMInnerReadOnlyAccess kepada pengguna.

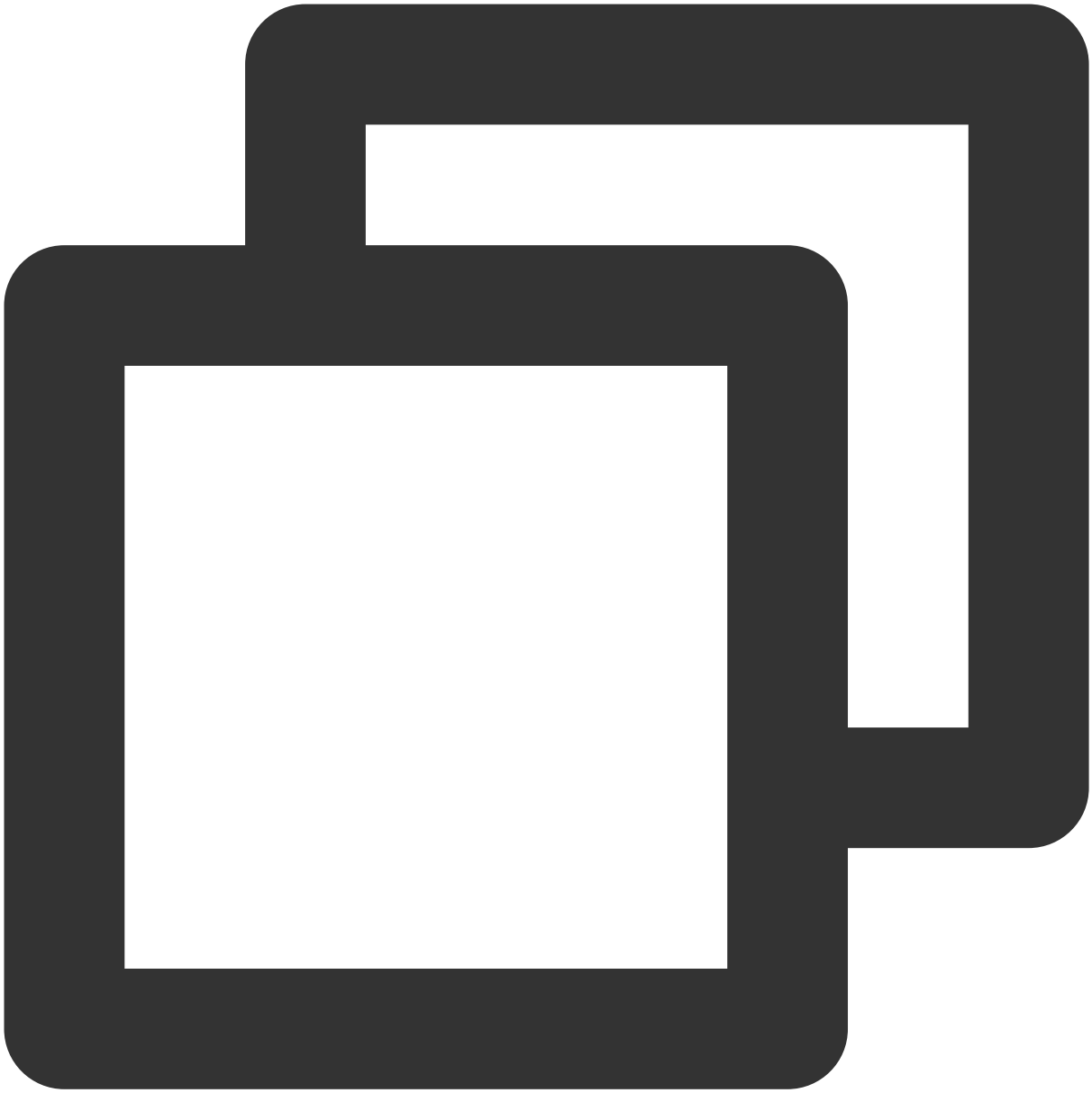
### Hanya baca (CVM dan sumber daya terkait)

Jika Anda ingin mengizinkan pengguna untuk hanya membuat kueri, tetapi tidak membuat, menghapus, atau memulai/mematikan instans CVM dan sumber daya terkait (VPC dan CLB), kaitkan pengguna dengan kebijakan bernama QcloudCVMReadOnlyAccess. Kebijakan ini dirancang untuk memberikan izin kepada pengguna untuk melakukan operasi berikut:
Semua operasi dimulai dengan "Describe" (Jelaskan) dan "Inquiry" (Pertanyaan) di CVM.
Semua operasi dimulai dengan "Describe" (Jelaskan), "Inquiry" (Pertanyaan), dan "Get" (Dapatkan) di VPC.
Semua operasi dimulai dengan "Describe" (Jelaskan) di CLB.

Semua operasi di Monitor.
Langkah-langkah detailnya adalah sebagai berikut:
Lihat Pengelolaan Otorisasi untuk petunjuk tentang cara memberikan kebijakan prasetel QcloudCVMReadOnlyAccess kepada pengguna.

### Kebijakan CBS

Jika Anda ingin mengizinkan pengguna untuk melihat, membuat, dan menggunakan disk cloud di konsol CVM, tambahkan operasi berikut ke kebijakan Anda dan kaitkan kebijakan dengan pengguna.
**CreateCbsStorages:** (CreateCbsStorages:) membuat disk cloud.
**AttachCbsStorages:** (AttachCbsStorages:) pasang disk cloud yang ditentukan ke CVM yang ditentukan.
**DetachCbsStorages:** (DetachCbsStorages:) lepaskan disk cloud yang ditentukan.
**ModifyCbsStorageAttributes:** (ModifyCbsStorageAttributes:) mengubah nama atau ID proyek dari disk cloud yang ditentukan.
**DescribeCbsStorages:** (DescribeCbsStorages:) menanyakan detail disk cloud.
**DescribeInstancesCbsNum:** (DescribeInstancesCbsNum:) menanyakan jumlah disk cloud yang dipasang dari CVM dan jumlah maksimum disk cloud yang diizinkan untuk dipasang ke CVM.
**RenewCbsStorage:** (RenewCbsStorage:) memperbarui disk cloud yang ditentukan.
**ResizeCbsStorage:** (ResizeCbsStorage:) mengubah ukuran disk cloud yang ditentukan.
Langkah-langkah detailnya adalah sebagai berikut:
1. Lihat Kebijakan untuk informasi dan buat kebijakan khusus yang memberikan izin untuk melihat informasi disk cloud di konsol CVM dan untuk membuat dan menggunakan disk cloud.
Gunakan berikut ini sebagai referensi sintaksis:



```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action": [
             "name/cvm:CreateCbsStorages",
             "name/cvm:AttachCbsStorages",
             "name/cvm:DetachCbsStorages",
             "name/cvm:ModifyCbsStorageAttributes",
             "name/cvm:DescribeCbsStorages"
```

```
            ],
            "resource": [
                "qcs::cvm::uin/1410643447:*"
            ]
        }
    ]
}
```

2. Temukan kebijakan yang dibuat, dan di kolom “Action” (Tindakan) pada baris tersebut, klik **Associate User/Group** (Kaitkan Pengguna/Grup).

3. Di jendela “Associate User/Group” (Kaitkan Pengguna/Grup), pilih pengguna/grup yang ingin Anda kaitkan, dan klik **OK** (OKE).

### Kebijakan grup keamanan

Untuk mengizinkan pengguna melihat dan menggunakan grup keamanan di konsol CVM, tambahkan operasi berikut ke kebijakan Anda, dan kaitkan kebijakan dengan pengguna.

**DeleteSecurityGroup:** (DeleteSecurityGroup:) menghapus grup keamanan.

**ModifySecurityGroupPolicys:** (ModifySecurityGroupPolicys:) mengganti semua kebijakan grup keamanan.

**ModifySingleSecurityGroupPolicy:** (ModifySingleSecurityGroupPolicy:) mengubah satu kebijakan grup keamanan.

**CreateSecurityGroupPolicy:** (CreateSecurityGroupPolicy:) membuat kebijakan grup keamanan.

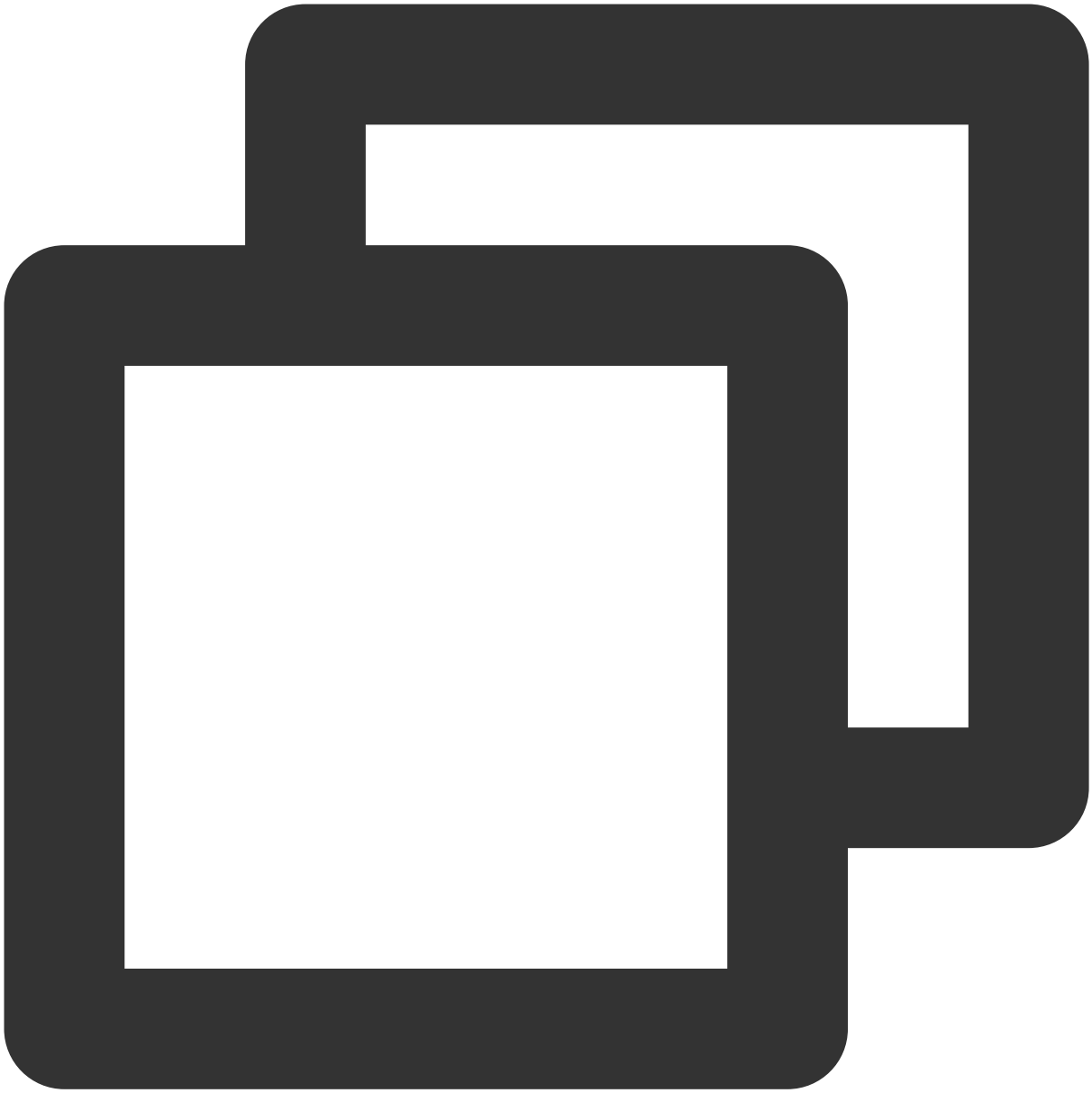
**DeleteSecurityGroupPolicy:** (DeleteSecurityGroupPolicy:) menghapus kebijakan grup keamanan.

**ModifySecurityGroupAttributes:** (ModifySecurityGroupAttributes:) mengubah atribut grup keamanan.

Langkah-langkah detailnya adalah sebagai berikut:

1. Lihat Kebijakan untuk mengetahui informasi dan buat kebijakan khusus yang memberikan izin untuk membuat, menghapus, dan mengubah grup keamanan di konsol CVM.

Gunakan berikut ini sebagai referensi sintaksis:



```
{
 "version": "2.0",
 "statement": [
     {
         "action": [
             "name/cvm:ModifySecurityGroupPolicys",
             "name/cvm:ModifySingleSecurityGroupPolicy",
             "name/cvm:CreateSecurityGroupPolicy",
             "name/cvm:DeleteSecurityGroupPolicy"
         ],
         "resource": "*",
```

```
            “effect": "allow"
        }
    ]
}
```

2. Temukan kebijakan yang dibuat, dan di kolom “Action” (Tindakan) pada baris tersebut, klik **Associate User/Group** (Kaitkan Pengguna/Grup).

3. Di jendela “Associate User/Group” (Kaitkan Pengguna/Grup), pilih pengguna/grup yang ingin Anda otorisasi, dan klik **OK** (OKE).

### Kebijakan untuk EIP

Jika Anda ingin mengizinkan pengguna untuk melihat dan menggunakan EIP di konsol CVM, tambahkan operasi berikut ke kebijakan Anda, dan kaitkan kebijakan dengan pengguna.

**AllocateAddresses:** (AllocateAddresses:) menetapkan EIP ke instans VPC atau CVM.

**AssociateAddress:** (AssociateAddress:) mengaitkan EIP dengan instans atau antarmuka jaringan.

**DescribeAddresses:** (DescribeAddresses:) melihat EIP di konsol CVM.

**DisassociateAddress:** (DisassociateAddress:) memisahkan EIP dari instans atau antarmuka jaringan.

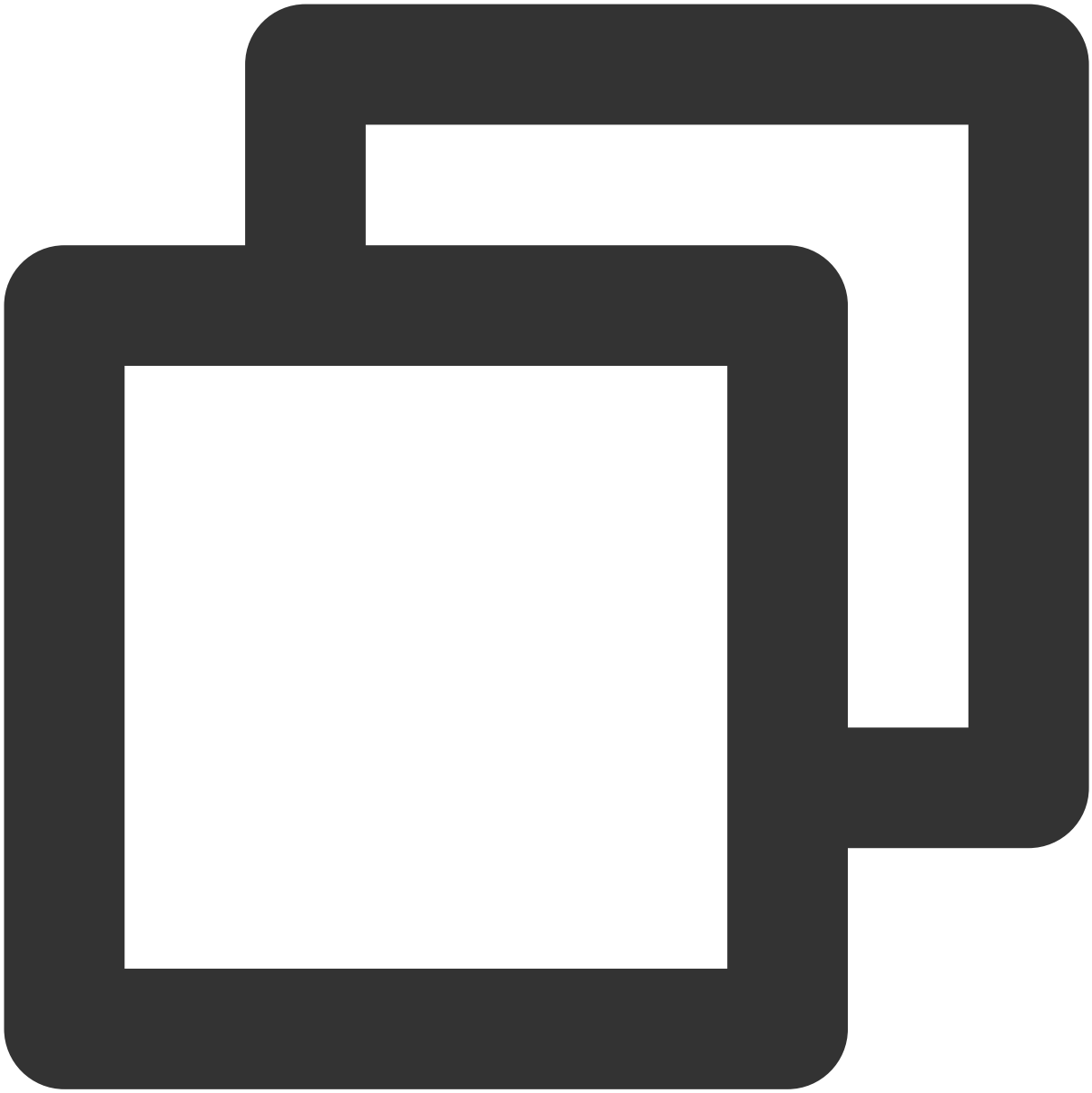
**ModifyAddressAttribute:** (ModifyAddressAttribute) mengubah atribut EIP.

**ReleaseAddresses:** (ReleaseAddresses:) merilis EIP.

Langkah-langkah detailnya adalah sebagai berikut:

1. Lihat Kebijakan untuk mengetahui informasi dan buat kebijakan kustom.

Kebijakan ini memungkinkan pengguna untuk melihat EIP dan menetapkannya serta mengaitkannya dengan instans di konsol CVM. Pengguna tidak dapat mengubah atribut EIP, memisahkannya dari instans, atau melepaskan EIP. Gunakan berikut ini sebagai referensi sintaksis:



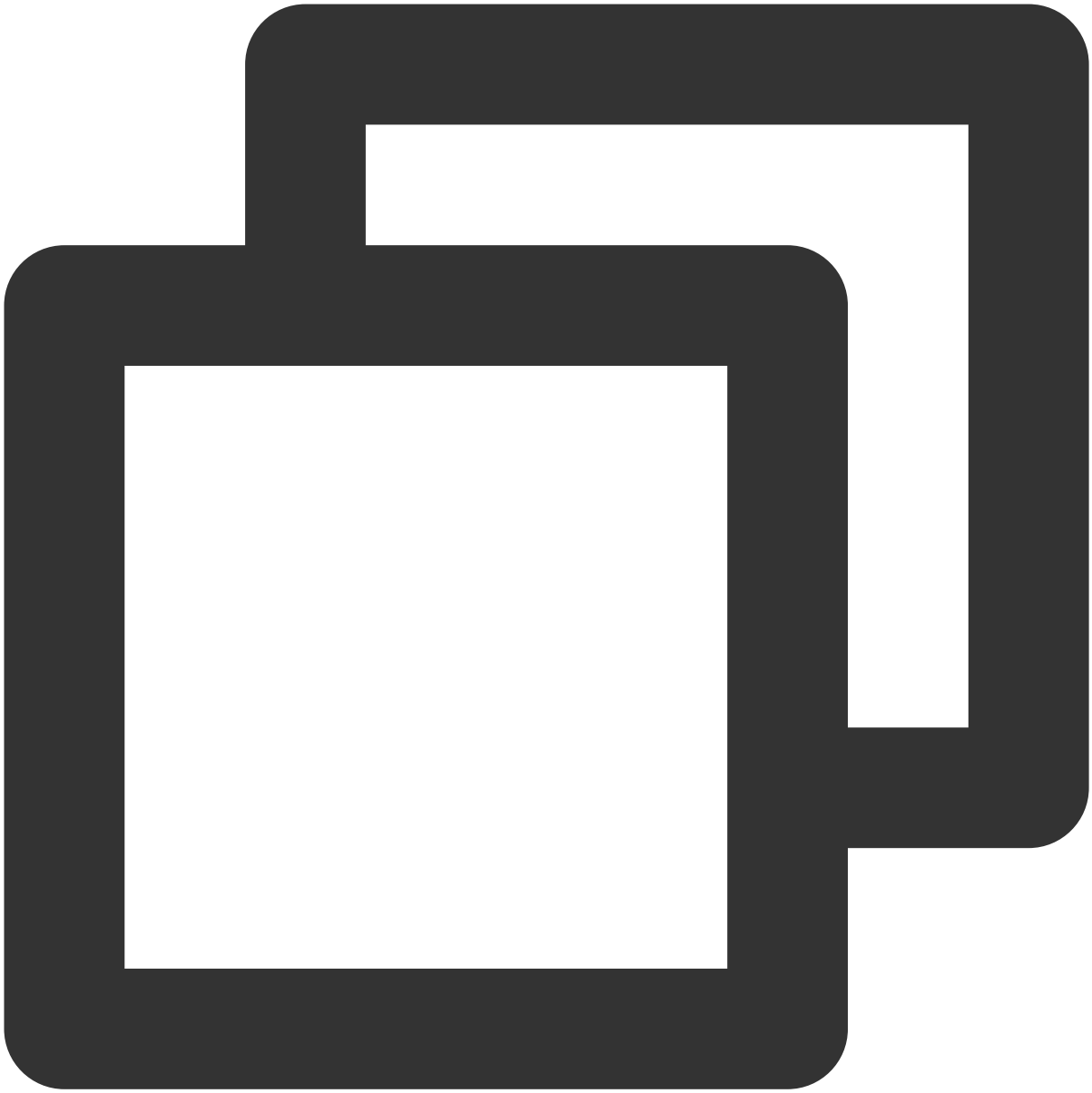
```
{
 "version": "2.0",
 "statement": [
     {
         "action": [
             "name/cvm:DescribeAddresses",
             "name/cvm:AllocateAddresses",
             "name/cvm:AssociateAddress"
         ],
         "resource": "*",
         “effect": "allow"
```

```
        }
    ]
}
```

2. Temukan kebijakan yang dibuat, dan di kolom “Action” (Tindakan) pada baris tersebut, klik **Associate User/Group** (Kaitkan Pengguna/Grup).
3. Di jendela “Associate User/Group” (Kaitkan Pengguna/Grup), pilih pengguna/grup yang ingin Anda otorisasi, dan klik **OK** (OKE).

### Kebijakan untuk mengizinkan pengguna melakukan operasi pada CVM tertentu

Jika Anda ingin mengotorisasi pengguna untuk melakukan operasi pada CVM tertentu, kaitkan kebijakan berikut dengan pengguna. Langkah-langkah detailnya adalah sebagai berikut:
1. Lihat Kebijakan untuk mengetahui informasi dan buat kebijakan kustom.
Kebijakan ini mengizinkan pengguna untuk mengoperasikan instans CVM dengan ID ins-1 di wilayah Guangzhou. Gunakan berikut ini sebagai referensi sintaksis:

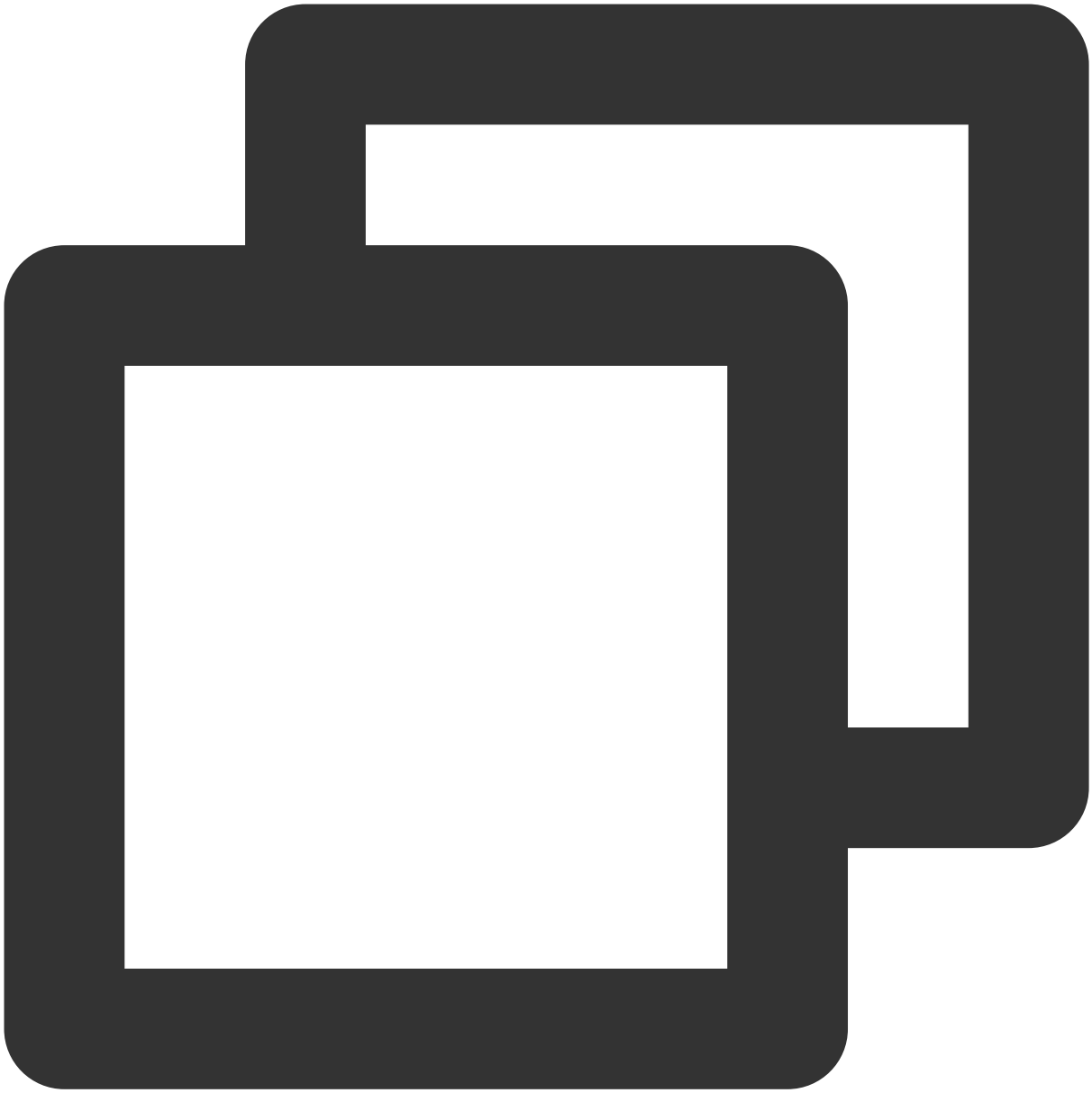


```
{
 "version": "2.0",
 "statement": [
     {
         "action": "cvm:*",
         "resource": "qcs::cvm:ap-guangzhou::instance/ins-1",
         “effect": "allow"
     }
 ]
}
```

2. Temukan kebijakan yang dibuat, dan di kolom “Action” (Tindakan) pada baris tersebut, klik **Associate User/Group** (Kaitkan Pengguna/Grup).
3. Di jendela “Associate User/Group” (Kaitkan Pengguna/Grup), pilih pengguna/grup yang ingin Anda otorisasi, dan klik **OK** (OKE).

### Kebijakan untuk mengizinkan pengguna melakukan operasi pada CVM di wilayah tertentu

Jika Anda ingin mengizinkan pengguna melakukan operasi pada CVM di wilayah tertentu, kaitkan kebijakan berikut dengan pengguna. Langkah-langkah detailnya adalah sebagai berikut:
1. Lihat Kebijakan untuk mengetahui informasi dan buat kebijakan khusus.
Kebijakan ini mengizinkan pengguna mengoperasikan instans CVM di wilayah Guangzhou. Gunakan berikut ini sebagai referensi sintaksis:

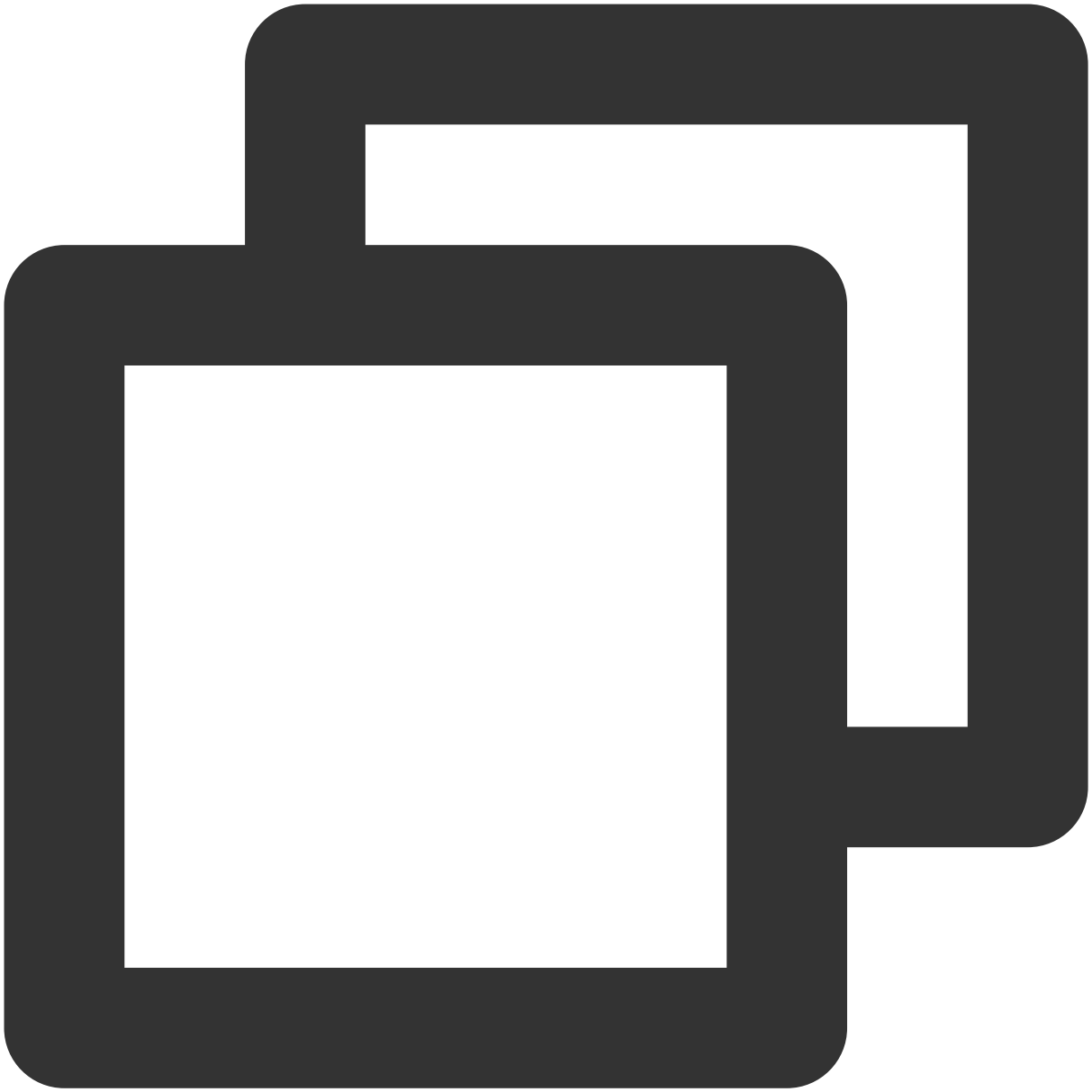


```
{
 "version": "2.0",
 "statement": [
     {
         "action": "cvm:*",
         "resource": "qcs::cvm:ap-guangzhou::*",
         “effect": "allow"
     }
 ]
}
```

2. Temukan kebijakan yang dibuat, dan di kolom “Action” (Tindakan) pada baris tersebut, klik **Associate User/Group** (Kaitkan Pengguna/Grup).
3. Di jendela “Associate User/Group” (Kaitkan Pengguna/Grup), pilih pengguna/grup yang ingin Anda otorisasi, dan klik **OK** (OKE).

### Memberikan sub-akun semua izin ke instans CVM kecuali pembayaran

Asumsikan bahwa akun CompanyExample, dengan ownerUin12345678, memiliki sub-akun yang disebut Pengembang. Pengembang memerlukan izin pengelolaan penuh (termasuk semua operasi seperti pembuatan dan pengelolaan) untuk instans CVM, kecuali pembayaran, yang berarti Pengembang dapat membuat pesanan tetapi tidak dapat membayarnya.
Anda dapat melakukannya dengan menggunakan salah satu dari dua solusi berikut:
**Solution A** (Solusi A)
Pemilik akun CompanyExample mengaitkan kebijakan prasetel QcloudCVMFullAccess dengan Pengembang. Untuk informasi selengkapnya, rujuk kepada Pengelolaan Otorisasi.
**Solution B** (Solusi B)
1.1 Gunakan berikut ini sebagai referensi sintaksis dan buat kebijakan kustom.



```
 {
"version": "2.0",
"statement":[
     {
         "effect": "allow",
         "action": "cvm:*",
         "resource": "*"
     }
]
}
```

1.2 Kaitkan kebijakan ke sub-akun. Untuk informasi selengkapnya, lihat Pengelolaan Otorisasi.

### Memberikan sub-akun izin untuk mengelola proyek

Asumsikan bahwa akun perusahaan, CompanyExample, dengan ownerUin 12345678, memiliki sub-akun yang disebut Pengembang. Pemilik CompanyExample ingin mengizinkan Pengembang mengelola proyek, termasuk menetapkan dan menghapus sumber daya, di konsol.
Langkah-langkah detailnya adalah sebagai berikut:
1. Buat kebijakan khusus untuk pengelolaan proyek.
Untuk informasi selengkapnya, lihat Kebijakan.
2. Lihat Pengelolaan Otorisasi untuk informasi tentang cara mengaitkan kebijakan kustom dengan sub-akun.
Jika Anda mengalami masalah izin saat mencoba melihat snapshot, citra, dan EIP, kaitkan kebijakan prasetel QcloudCVMAccessForNullProject, QcloudCVMOrderAccess, dan QcloudCVMLaunchToVPC dengan sub-akun.
Untuk informasi selengkapnya tentang otorisasi, lihat Pengelolaan Otorisasi.

### Kebijakan kustom

Jika kebijakan prasetel tidak dapat memenuhi persyaratan Anda, Anda dapat membuat kebijakan kustom.
Untuk petunjuk mendetail, lihat Kebijakan.
Untuk informasi selengkapnya tentang sintaksis kebijakan CVM, lihat Sintaksis Kebijakan Otorisasi.