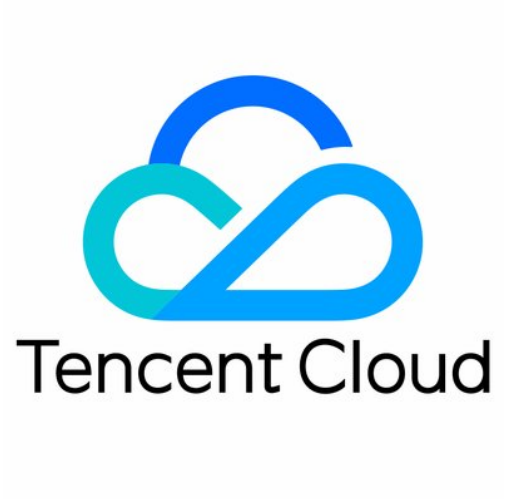
Virtual Private Cloud

Panduan Operasi

Dokumen produk



Direktori dokumen

Panduan Operasi
Topologi Jaringan

Waktu update terbaru：2024-01-24 17:48:51

Peta topologi jaringan menampilkan semua sumber informasi VPC, sehingga Anda dapat memperoleh deployment dan koneksi VPC secara real time.

Petunjuk

1. Login ke Konsol VPC.
2. Klik **Network Topology Map** (Peta Topologi Jaringan) di bilah sisi kiri.
3. Pilih wilayah dan VPC untuk melihat sumber informasi cloud VPC seperti CVM, CLB, TencentDB, dan NoSQL, dan relasi topologi jaringannya.
Dalam dua subnet sampel VPC seperti yang ditampilkan di bawah ini, subnet `test6` berisi dua instans CLB. VPC ini berkomunikasi dengan Internet melalui NAT Gateway dan CLB jaringan publik. Ini berkomunikasi dengan VPC yang berlawanan melalui peering connection.

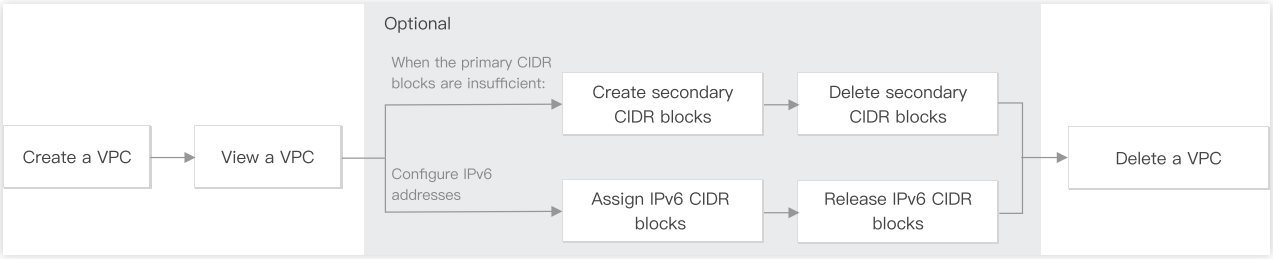
Virtual Private Cloud (VPC)
Ikhtisar

Waktu update terbaru：2024-01-24 17:48:51

VPC adalah jaringan virtual yang terisolasi secara logis yang dapat Anda gunakan secara eksklusif dan direncanakan secara mandiri di Tencent Cloud. Untuk menggunakan sumber informasi Tencent Cloud, Anda harus membuat VPC dan subnet. Subnet adalah ruang jaringan di VPC. Anda setidaknya dapat membagi VPC menjadi satu subnet. VPC bersifat regional, sedangkan subnet dikhususkan untuk zona ketersediaan. Subnet di VPC yang sama dapat berkomunikasi satu sama lain melalui jaringan pribadi secara default.
Semua sumber informasi cloud seperti CVM dan CLB dalam VPC harus di-deploy di subnet.

Siklus Pemakaian VPC

Siklus pemakaian VPC berbeda-beda sesuai dengan kebutuhan, seperti yang ditampilkan di bawah ini:



1. Membuat VPC: Anda harus berhati-hati merencanakan jaringan Anda sebelum membuat VPC. Blok CIDR dari VPC dan subnet tidak dapat diubah setelah dibuat.
2. Melihat VPC: Anda dapat melihat informasi dasar VPC, hubungan CCN-nya, dan sumber informasi yang dikandungnya.
3. (Opsional) Pilih operasi yang berlaku untuk kasus penggunaan Anda:
Jika blok CIDR utama tidak mencukupi, lihat Mengedit Blok CIDR IPv4:
Membuat blok CIDR sekunder: Anda dapat membuat blok CIDR sekunder untuk memenuhi permintaan jaringan Anda secara aktual.
Menghapus blok CIDR sekunder: Anda dapat menghapus blok CIDR sekunder jika Anda tidak lagi membutuhkannya.
4. Menghapus VPC: setelah VPC dihapus, subnet dan tabel rutenya juga dihapus.

Batasan

Waktu update terbaru：2024-01-24 17:48:51

Batasan penggunaan

Rentang IP VPC dan subnet tidak dapat diubah setelah dibuat.
Untuk setiap subnet, Tencent Cloud mencadangkan dua IP pertama dan yang terakhir untuk jaringan IP. Misalnya, jika blok CIDR subnet adalah `172.16.0.0/24`, maka `172.16.0.0`, `172.16.0.1`, dan `172.16.0.255` dicadangkan oleh Tencent Cloud.
Saat Anda menambahkan CVM ke VPC, instans akan ditetapkan secara acak dengan IP pribadi dari subnet yang ditentukan. Anda dapat menetapkan ulang IP pribadi setelah instans dibuat.
Di VPC, IP pribadi CVM sesuai dengan satu alamat IP publik.
CVM berbasis jaringan klasik tidak dapat terhubung dengan sumber informasi cloud di blok CIDR sekunder.
Peering connection tidak mendukung blok CIDR sekunder.
Cloud Connect Network, VPN gateway, dan standard direct connect gateway mendukung blok CIDR sekunder.

Batasan kuota

Sumber Informasi	Batas
Jumlah instans VPC per wilayah per akun	20
Jumlah subnet per VPC	100
Jumlah blok CIDR sekunder per VPC	5

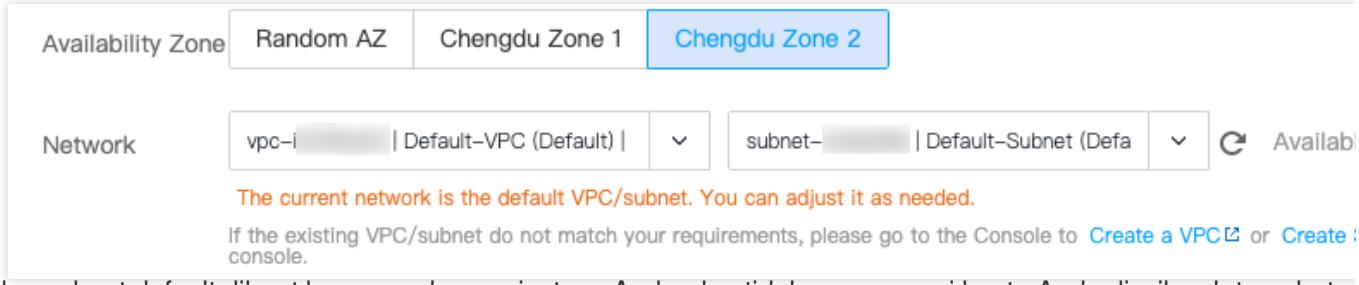
Keterangan:

Jika Anda ingin meningkatkan kuota, harap kirim tiket untuk mendaftar.

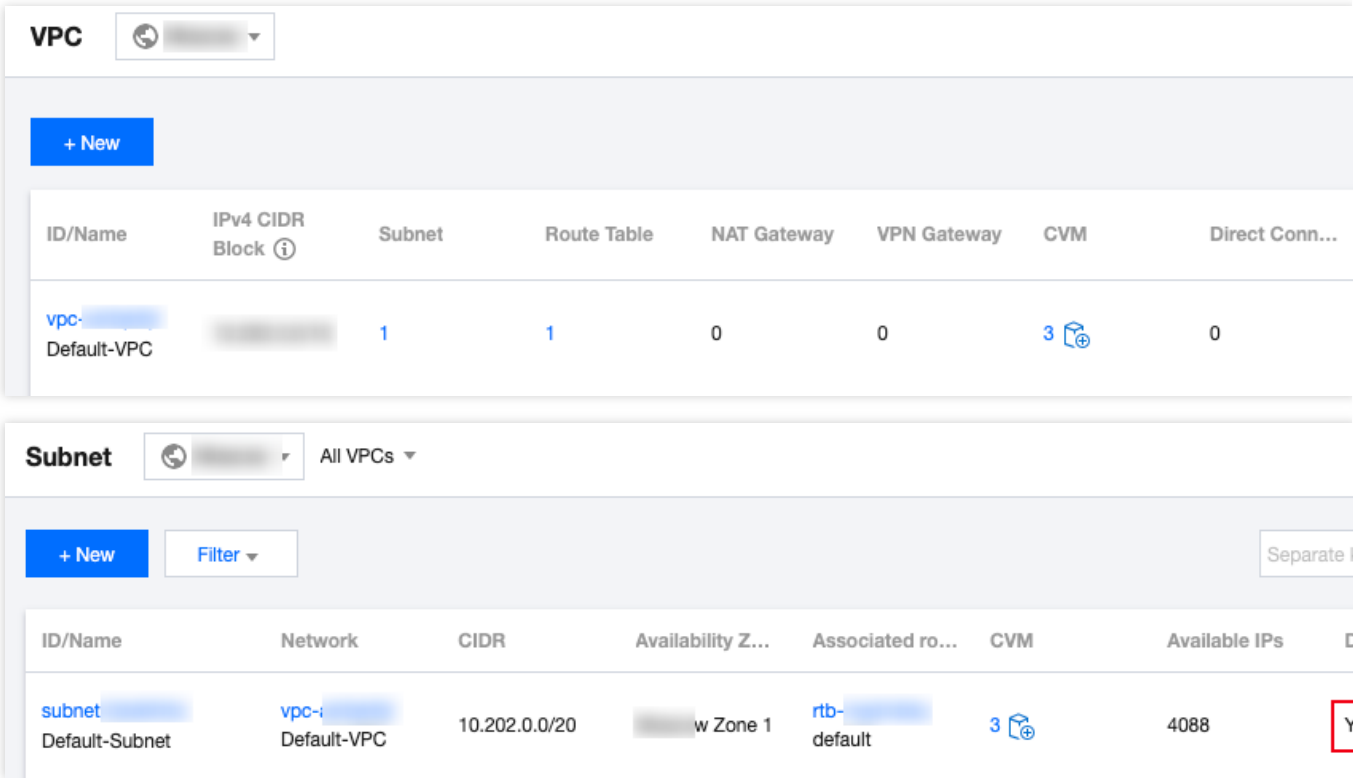
Membuat VPC

Waktu update terbaru：2024-01-24 17:48:51

Virtual Private Cloud (VPC) adalah dasar untuk menggunakan layanan Tencent Cloud. Saat membeli instans seperti CVM, CLB, atau TencentDB di wilayah yang belum memiliki VPC, VPC dan subnet default akan dibuat secara otomatis.



VPC dan subnet default dibuat bersama dengan instans Anda, dan tidak mengurangi kuota Anda di wilayah tersebut. Mereka bekerja sama seperti yang dibuat secara manual. Hanya ada satu VPC dan subnet default di setiap wilayah. Anda dapat menghapus VPC dan subnet default jika Anda tidak lagi membutuhkannya.



Anda dapat merujuk ke dokumen ini untuk membuat instans VPC di konsol jika VPC default atau yang sudah ada tidak sesuai.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih wilayah di bagian atas halaman **VPC**, dan klik **+New** (+Baru).
3. Masukkan informasi VPC dan informasi subnet di pop-up **Create VPC** (Buat VPC).

Keterangan:

Blok CIDR dari VPC dan subnet tidak dapat diubah setelah dibuat.

Blok CIDR VPC dapat berupa salah satu dari rentang IP berikut. Agar VPC dapat berkomunikasi satu sama lain melalui jaringan pribadi, blok CIDR-nya tidak boleh tumpang tindih.

`10.0.0.0` - `10.255.255.255` (rentang mask antara 16 hingga 28)

`172.16.0.0` - `172.31.255.255` (rentang mask antara 16 hingga 28)

`192.168.0.0` - `192.168.255.255` (rentang mask antara 16 hingga 28)

Blok CIDR subnet harus berada di dalam atau sama dengan blok CIDR VPC.

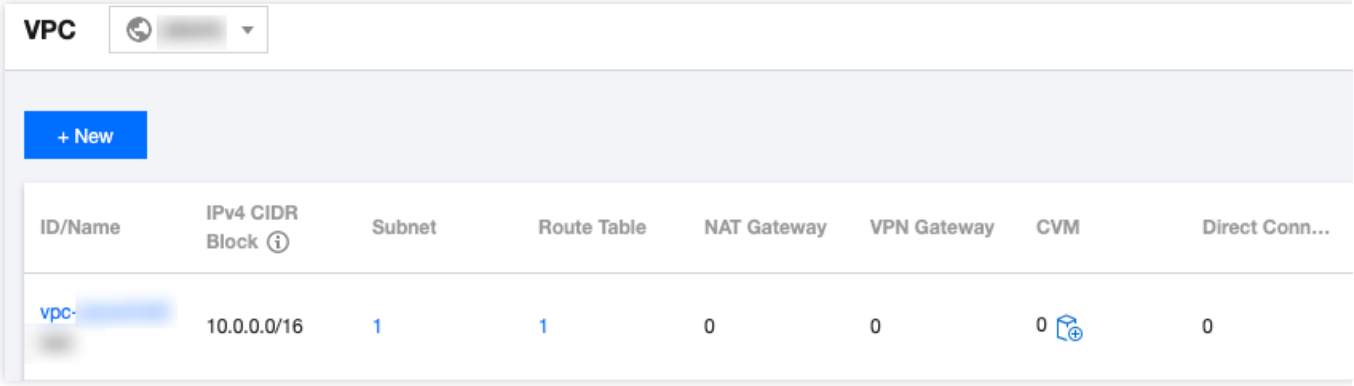
Misalnya, jika rentang IP VPC adalah `10.0.0.0/16` , maka rentang IP subnetnya dapat berupa `10.0.0.0/16` , `10.0.0.0/24` , dll.

Zona ketersediaan: subnet khusus untuk zona ketersediaan. Pilih zona ketersediaan tempat subnet berada. VPC memungkinkan subnet di zona ketersediaan yang berbeda dan secara default subnet ini dapat berkomunikasi satu sama lain melalui jaringan pribadi.

Tabel rute yang terhubung: subnet harus dihubungkan dengan tabel rute untuk penerusan lalu lintas. Tabel rute default akan dikaitkan untuk memastikan interkoneksi jaringan pribadi di VPC.

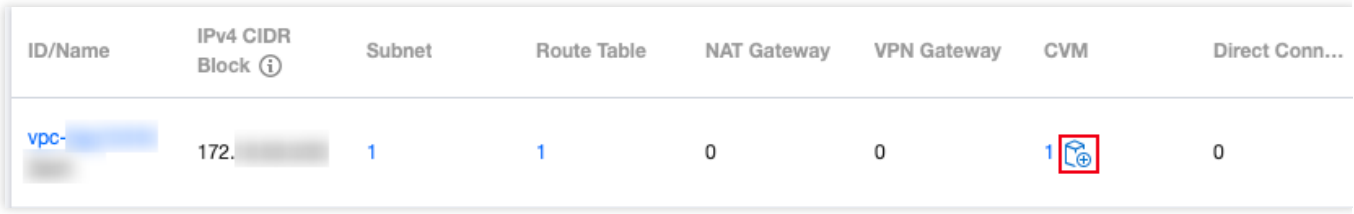
Opsi lanjutan: Anda dapat menambahkan tag untuk mengelola izin sumber informasi sub-pengguna dan kolaborator dengan lebih baik.

4. Setelah konfigurasi selesai, klik **OK** (Oke). VPC yang berhasil dibuat akan ditampilkan dalam daftar, seperti yang ditampilkan di bawah ini. VPC baru memiliki subnet dan tabel rute default.



Operasi Berikutnya

Setelah VPC dan subnet dibuat, Anda dapat men-deploy sumber informasi termasuk CVM dan CLB di dalam VPC. Klik ikon seperti ditunjukkan gambar di bawah ini untuk langsung membeli CVM di halaman pembelian CVM. Untuk informasi selengkapnya, lihat Membangun VPC IPv4.



Melihat VPC

Waktu update terbaru：2024-01-24 17:48:51

Anda dapat mengkueri semua sumber informasi VPC melalui konsol VPC, seperti sumber informasi cloud dan koneksi di VPC.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC**. Anda dapat memeriksa informasi semua VPC di wilayah ini dalam daftar.

Kolom	Deskripsi
ID/Nama	ID dan nama VPC. Nama dapat dimodifikasi.
Blok CIDR IPv4	Blok CIDR IPv4 dari VPC. Itu tidak dapat dimodifikasi.
Blok CIDR IPv6	Blok CIDR IPv6 dari VPC. Fitur ini saat ini dalam versi beta. Untuk menggunakannya, harap kirim tiket.
Subnet	Jumlah subnet di VPC. Klik nomor untuk mengakses halaman **Subnet**.
Tabel Rute	Jumlah tabel rute di VPC. Klik nomor untuk mengakses halaman **Tabel Rute**.
NAT Gateway	Jumlah NAT Gateway di VPC. Klik nomor untuk mengakses halaman **NAT Gateway**.
VPN Gateway	Jumlah VPN gateway di VPC. Klik nomor untuk mengakses halaman **VPN Gateway**.
CVM	Jumlah CVM di VPC. Klik nomor untuk mengakses halaman CVM. Klik ikon CVM untuk mengarahkan ke halaman pembelian CVM.
Classiclink	Jumlah instans CVM berbasis jaringan klasik yang terhubung dengan VPC ini. CVM berbasis jaringan klasik hanya dapat dihubungkan dengan satu VPC.
Direct Connect Gateway	Jumlah direct connect gateway di VPC. Klik nomor untuk mengakses halaman Direct Connect Gateway.
Default VPC	Menunjukkan apakah VPC adalah VPC default wilayah. Hanya ada satu VPC default di wilayah. VPC default dibuat secara otomatis saat Anda membeli sumber informasi seperti CVM. Ini bekerja sama seperti yang dibuat secara manual.
Waktu Pembuatan	Waktu VPC dibuat.

Operasi	Operasi VPC yang didukung. Hanya VPC tanpa sumber informasi apa pun yang dapat dihapus. Anda dapat mengeklik **Lainnya** untuk mengedit blok CIDR IPv4 dan blok CIDR IPv6 jika berlaku.

3. Klik ID VPC untuk melihat detail, termasuk informasi dasar, hubungan CCN, dan sumber informasi yang terhubung. Klik nomor di sebelah sumber informasi untuk mengakses halaman pengelolaan sumber informasi.
4. Kembali ke daftar VPC, dan klik di kotak pencarian di sudut kanan atas untuk memfilter VPC menurut atribut sumber informasi yang berbeda.
5. Klik ikon pengaturan di sudut kanan atas untuk menyesuaikan kolom tampilan.

Mengedit Blok CIDR IPv4

Waktu update terbaru：2024-01-24 17:48:51

Setiap VPC dapat memiliki satu blok CIDR utama, yang tidak dapat dimodifikasi setelah pembuatan VPC. Saat IP di blok CIDR primer tidak dapat memenuhi kebutuhan Anda, Anda dapat membuat beberapa blok CIDR sekunder untuk menambahkan rentang IP.
Anda dapat mengalokasikan subnet dengan rentang IP dari blok CIDR utama atau sekunder. Semua subnet dari VPC yang sama saling terhubung secara default, terlepas dari apakah subnet termasuk dalam blok CIDR utama atau sekunder.

Batas Penggunaan

CVM berbasis jaringan klasik tidak dapat terhubung dengan sumber daya cloud di blok CIDR sekunder.
Peering connection tidak mendukung blok CIDR sekunder.
Cloud Connect Network, VPN gateway, dan standard direct connect gateway mendukung blok CIDR sekunder.
Perhatikan batasan berikut untuk direct connect gateway:
Fitur ini tidak tersedia di wilayah Finance Cloud.
Hingga 10 blok CIDR sekunder dapat disebarkan.
Fitur ini tidak tersedia untuk NAT direct connect gateway.

Membuat Blok CIDR Sekunder

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC** (VPC).
3. Di daftar VPC, cari VPC dan pilih **More** > **Edit IPv4 CIDR block** (Lainnya > Edit blok CIDR IPv4) pada kolom **Operation** (Operasi).
4. Di kotak dialog pop-up, klik **Add** (Tambahkan) untuk memasukkan blok CIDR sekunder.

Perhatian:

Blok CIDR sekunder dapat tumpang tindih dengan rentang IP tujuan dari rute kustom. Perhatikan bahwa blok CIDR sekunder menggunakan rute lokal, yang memiliki prioritas lebih tinggi daripada rute subnet kustom.

5. Klik **OK** (OKE).

Menghapus Blok CIDR Sekunder

1. Login ke Konsol VPC.

2. Pilih wilayah VPC di bagian atas halaman **VPC** (VPC).
3. Di daftar VPC, temukan VPC tempat blok CIDR sekunder akan dihapus, dan pilih **More** > **Edit IPv4 CIDR block** (Lainnya > Edit blok CIDR IPv4) pada kolom **Operation** (Operasi).
4. Di kotak dialog pop-up, klik **Delete** (Hapus) di sebelah blok CIDR sekunder.
5. Klik **OK** (OKE).

Menghubungkan atau Memutuskan Hubungan CCN

Waktu update terbaru：2024-01-24 17:48:51

Cloud Connect Network (CCN) menjembatani VPC Tencent Cloud dan antara VPC dan IDC lokal. Ini memberi Anda interkoneksi jaringan pribadi multipoint. Untuk memanfaatkan fitur CCN ini, Anda harus terlebih dahulu menambahkan VPC ke CCN. Dokumen ini menjelaskan cara menghubungkan VPC dengan atau memutuskan koneksinya dari CCN.

Menghubungkan dengan CCN

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC**.
3. Klik ID VPC untuk mengakses halaman **Basic Information** (Informasi Dasar).
4. Klik **Associate Now** (Hubungkan Sekarang) di bagian **Associate with CCN** (Hubungkan dengan CCN) untuk membuka kotak dialog **Associate with CCN** (Hubungkan dengan CCN).
5. Konfigurasikan parameter sebagai berikut.
Account (Akun): akun pemilik instans CCN. Instans VPC dan CCN dapat berada di bawah akun yang sama atau berbeda. Jika Anda memilih **Other accounts** (Akun lain), masukkan **Account ID** (ID Akun). Pemilik akun harus menerima permohonan CCN dalam waktu 7 hari, jika tidak, permohonan akan kedaluwarsa. Pemilik CCN menanggung biaya interkoneksi jaringan yang dihasilkan oleh instans yang terhubung ke CCN.
CCN ID (ID CCN): pilih ID CCN dari daftar pilihan untuk **My Account** (Akun Saya) atau masukkan ID CCN untuk **Other accounts** (Akun lain).
6. Klik **OK** (Oke). Maka statusnya akan menjadi **Connected** (Terhubung) seperti ditampilkan gambar di bawah ini.

Pemutusan koneksi dari CCN

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC**.
3. Temukan VPC yang akan diputuskan koneksinya dari CCN, dan klik ID VPC untuk mengakses halaman **Basic Information** (Informasi Dasar).
4. Klik **Disassociate** (Putuskan koneksi) di bagian **Associate with CCN** (Hubungkan dengan CCN).
5. Periksa kembali dan konfirmasikan risiko operasi dan klik **Disassociate** (Putuskan koneksi).

Operasi yang Relevan

Memodifikasi DNS VPC

Waktu update terbaru：2024-01-24 17:48:51

CVM di Tencent Cloud VPC mendukung DHCP. Opsi DHCP yang dapat dikonfigurasi termasuk alamat DNS dan nama domain. Dokumen ini menjelaskan cara mengubah alamat DNS dan nama domain VPC.

Keterangan:

Dynamic Host Configuration Protocol (DHCP) adalah protokol jaringan LAN yang mendefinisikan standar untuk mentransfer informasi konfigurasi ke server jaringan TCP/IP.

Untuk saat ini, VPC yang dibuat sebelum 1 April 2018 tidak mendukung fitur DHCP. Jika Anda tidak dapat mengubah alamat DNS dan nama domain di konsol, berarti VPC Anda tidak mendukung fitur ini.

Catatan

Konfigurasi baru akan berlaku pada semua CVM di VPC.

Untuk CVM yang baru dibuat, konfigurasi yang dimodifikasi langsung berlaku.

Untuk CVM yang ada, konfigurasi yang dimodifikasi berlaku setelah CVM atau layanan jaringan dimulai ulang.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC** (VPC).
3. Klik ID VPC untuk mengakses halaman **Basic Information** (Informasi Dasar).
4. Klik ikon edit untuk memodifikasi DNS dan nama domain masing-masing.

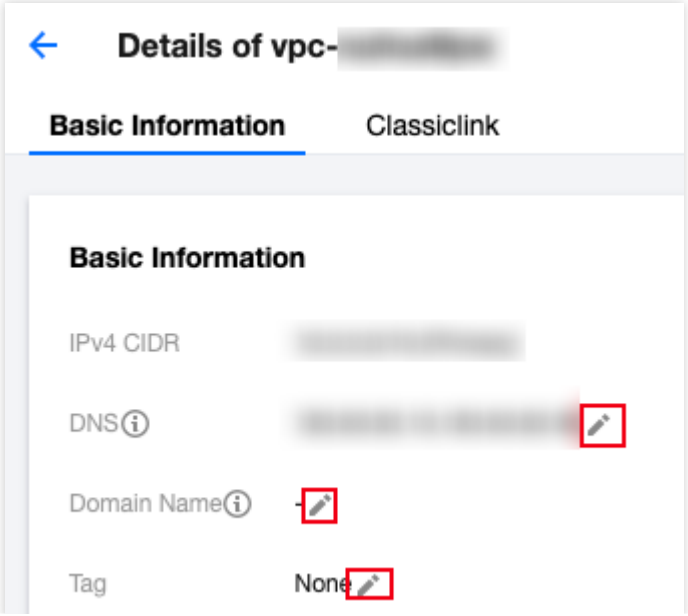
DNS: Alamat server DNS

Keterangan:

DNS default Tencent Cloud adalah “183.60.83.19” dan “183.60.82.98”. Jika DNS default tidak digunakan, layanan internal seperti aktivasi Windows, NTP, dan YUM tidak akan tersedia.

DNS mendukung maksimal empat alamat IP. Pisahkan IP dengan koma. Perhatikan bahwa sistem operasi tertentu mungkin tidak dapat mendukung empat alamat DNS.

Nama Domain: Akhiran nama host CVM, seperti “example.com”. Anda dapat memasukkan hingga 60 karakter, atau tetap menggunakan konfigurasi default jika Anda tidak memiliki persyaratan khusus.



Memodifikasi Nama dan Tag VPC

Waktu update terbaru：2024-01-24 17:48:52

Dokumen ini menjelaskan cara memodifikasi nama, tag, atau informasi lain dari VPC.

Petunjuk

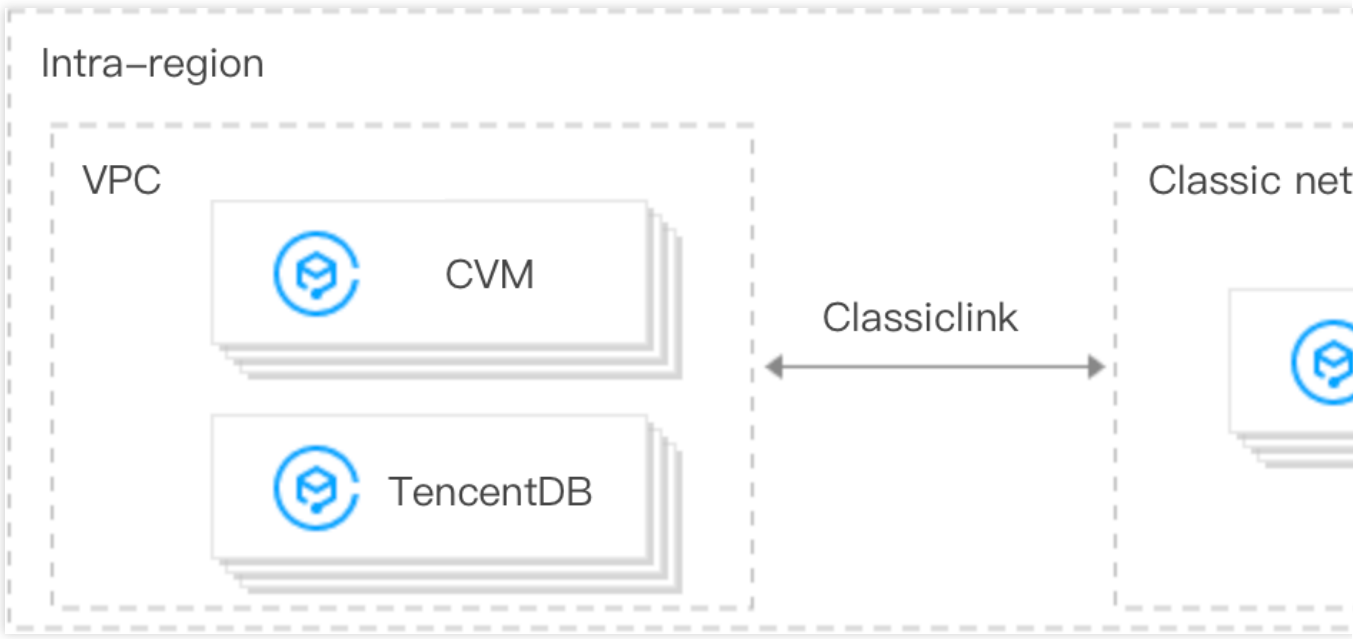
1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC** (VPC).
3. Klik ikon edit di sebelah nama VPC untuk memodifikasinya.
4. Klik ID VPC untuk mengakses halaman **Basic Information** (Informasi Dasar).
5. Tag digunakan untuk mengidentifikasi dan mengelola sumber informasi. Anda dapat mengeklik ikon edit untuk menambah atau menghapus tag.

Classiclink

Ikhtisar

Waktu update terbaru：2024-01-24 17:48:51

Fitur Classiclink memungkinkan CVM berbasis VPC berkomunikasi dengan CVM berbasis jaringan klasik. Misalnya, CVM berbasis jaringan klasik dapat berkomunikasi dengan sumber daya VPC seperti CVM, TencentDB, CLB jaringan pribadi, Redis/CMEM, dll.
Sumber daya VPC hanya dapat mengakses CVM berbasis jaringan klasik, tetapi tidak dapat mengakses sumber daya lain di jaringan klasik, seperti TencentDB dan CLB



Batas Penggunaan

VPC hanya dapat terhubung dengan jaringan klasik **in the same region** (di wilayah yang sama).
Rentang IP VPC harus berada dalam `10.0.0.0/16-10.47.0.0/16` (termasuk subset), jika tidak, mungkin ada konflik IP, yang dapat menyebabkan kegagalan saat menghubungkan dan berkomunikasi dengan CVM berbasis jaringan klasik.
CVM berbasis jaringan klasik hanya dapat dihubungkan dengan satu VPC dalam satu waktu.
Satu VPC mendukung hubungan dengan hingga 100 CVM berbasis jaringan klasik.
Setelah CVM jaringan klasik dihubungkan dengan VPC, CVM berbasis jaringan klasik hanya dapat berkomunikasi dengan sumber daya di blok CIDR primer daripada blok CIDR sekunder pada VPC.
Instans CLB dalam VPC tidak dapat diikat ke CVM berbasis jaringan klasik yang saling terhubung dengan VPC yang sama.

Dalam situasi Classiclink, lalu lintas CVM hanya dapat dirutekan ke alamat IP pribadi di dalam VPC daripada tujuan di luar VPC.

Keterangan:

CVM berbasis jaringan klasik tidak dapat mengakses sumber daya jaringan publik atau pribadi di luar VPC saat ini melalui perangkat jaringan seperti VPN gateway, gateway direct connect, public gateway, peering connection, dan NAT Gateway. Demikian juga, peer dari VPN gateway, direct connect gateway, dan peering connection tidak dapat mengakses CVM berbasis jaringan klasik.

Catatan

Mengubah IP pribadi CVM berbasis jaringan klasik akan membatalkan hubungannya dengan VPC, dan menyebabkan konfigurasi menjadi tidak valid. Untuk menghubungkannya, Anda perlu menambahkan Classiclink lagi di konsol VPC.

Classiclink tidak akan terpengaruh oleh tindakan yang diambil terkait CVM seperti isolasi karena pembayaran yang jatuh tempo, isolasi keamanan, migrasi cold, failover, modifikasi konfigurasi, dan peralihan sistem operasi.

CVM akan otomatis diputuskan hubungannya dari VPC jika CVM dikembalikan.

Referensi

Untuk informasi selengkapnya tentang cara mengoperasikan Classiclink, lihat Mengelola Classiclink.

Mengelola Classiclink

Waktu update terbaru：2024-01-24 17:48:51

Membuat Classiclink

Classiclink menghubungkan CVM berbasis jaringan klasik dengan VPC untuk mengaktifkan interkoneksi antara VPC dan jaringan klasik. Hal ini memungkinkan CVM berbasis jaringan klasik berkomunikasi dengan sumber daya VPC.

Keterangan:

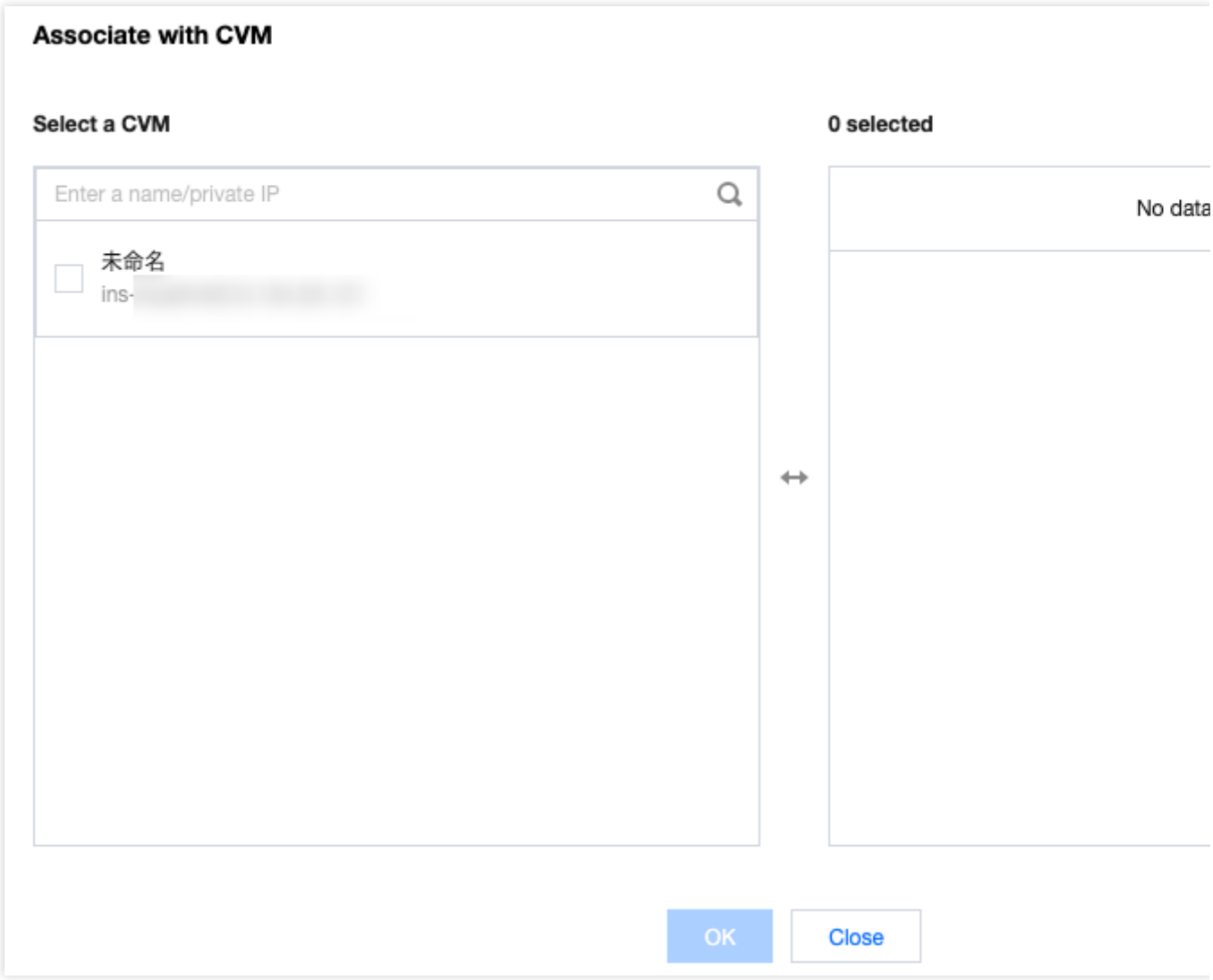
IP pribadi dari CVM berbasis jaringan klasik terkait akan secara otomatis ditambahkan ke kebijakan lokal untuk tabel rute VPC. Hal ini memungkinkan interkoneksi tanpa perlu memodifikasi kebijakan perutean VPC secara manual.

Setelah CVM berbasis jaringan klasik dihubungkan dengan VPC, pengaturan ACL firewall dan jaringannya akan tetap efektif.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih wilayah, dan klik ID VPC yang memerlukan Classiclink untuk mengakses halaman detail.
3. Klik tab **Classiclink** (Classiclink), lalu klik **+Associate with CVM** (+Hubungkan dengan CVM).

4. Pada jendela pop-up, pilih CVM di jaringan klasik untuk dihubungkan dengan VPC dan klik **OK** (OKE).

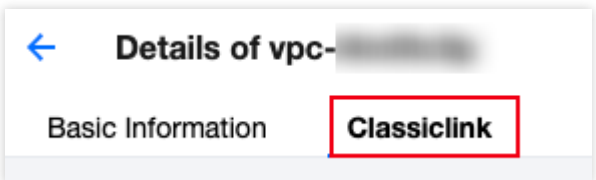


Melihat Classiclink

Anda dapat melihat daftar CVM berbasis jaringan klasik yang terhubung dengan VPC.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih wilayah, dan klik ID VPC yang memerlukan Classiclink untuk mengakses halaman detail.
3. Klik tab **Classiclink** (Classiclink) untuk melihat daftar CVM berbasis jaringan klasik yang terhubung dengan VPC.



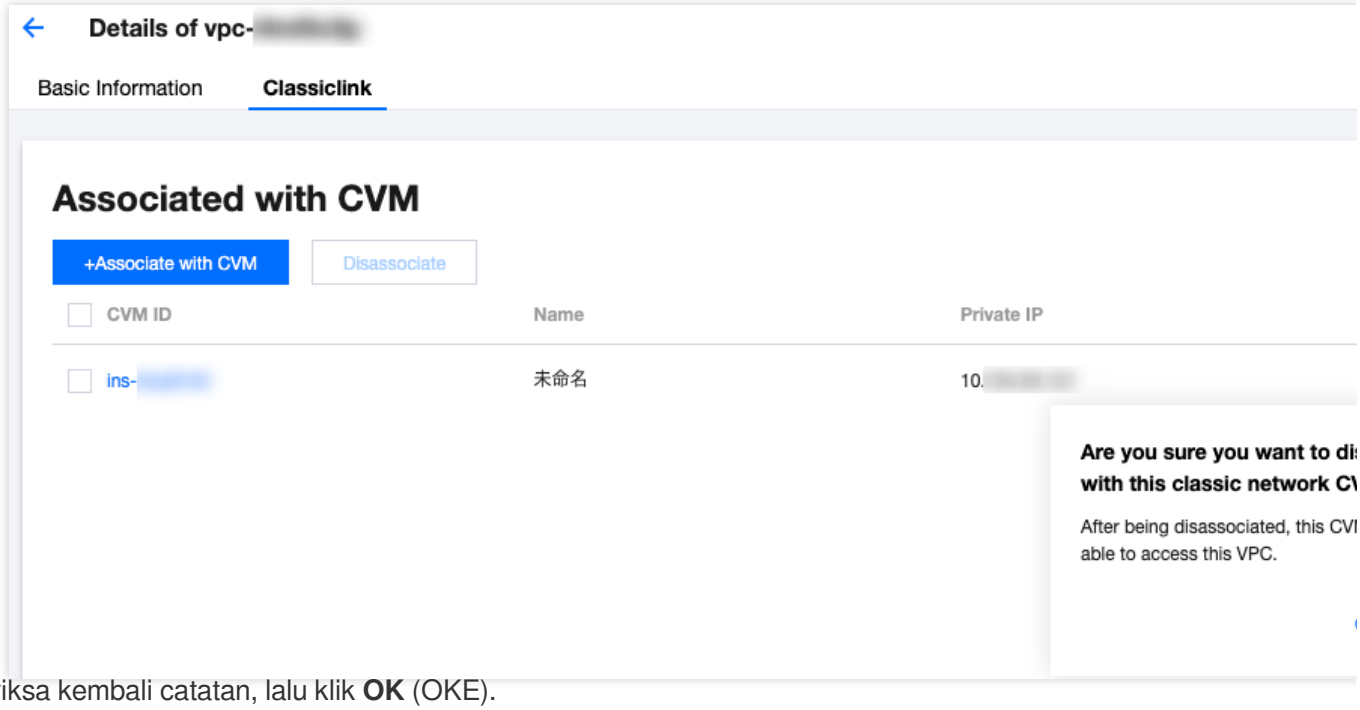
4. Masukkan IP pribadi pada kotak pencarian di sudut kanan atas untuk menemukan CVM dengan cepat.

Menghapus Classiclink

Tindakan ini akan memutuskan koneksi CVM berbasis jaringan klasik dari VPC dan menghentikan interkoneksinya.

Petunjuk

1. Login ke Konsol VPC.
2. Klik ID VPC yang memerlukan Classiclink untuk mengakses halaman detail.
3. Klik tab **Classiclink** (Classiclink), pilih CVM yang akan dibatalkan hubungannya dari daftar CVM berbasis jaringan klasik, lalu klik **Disassociate** (Batalkan Hubungan) di kolom **Operation** (Operasi).



4. Periksa kembali catatan, lalu klik **OK** (OKE).
5. Untuk membatalkan hubungan beberapa CVM, Anda dapat memilih CVM ini untuk dibatalkan hubungannya dan klik **Disassociate** (Batalkan Hubungan) di atas daftar.

Mengaktifkan atau Menonaktifkan Multicast

Waktu update terbaru：2024-01-24 17:48:52

Dokumen ini menjelaskan cara mengaktifkan atau menonaktifkan multicast untuk VPC.

Latar belakang

Broadcast dan multicast adalah mode komunikasi satu-ke-semuanya, yang dapat menghemat bisnis di bandwidth jaringan dan mengurangi beban jaringan melalui transmisi data efisien point-to-multipoint.
Dalam mode unicast, server yang memulai mengirimkan data ke N server secara terpisah. Jika multicast digunakan, server mengirimkan data yang sama ke N server hanya sekali, yang mengurangi konsumsi sumber informasi server serta sumber informasi bandwidth jaringan backbone.
Keterangan:
Fitur broadcast dan multicast saat ini dalam uji beta. Jika diperlukan, harap kirim tiket.
Saat ini wilayah yang mendukung multicast dan broadcast adalah: Beijing, Shanghai, Guangzhou, Chengdu, Chongqing, Nanjing, Hong Kong (Tiongkok), Singapura, Seoul, Tokyo, Bangkok, Toronto, Silicon Valley, Virginia, Frankfurt, dan Moscow.
Multicast: Tencent Cloud mendukung multicast pada dimensi VPC.
Broadcast: Tencent Cloud mendukung broadcast pada dimensi subnet.

Ikhtisar

Multicast dan broadcast sebagian besar digunakan dalam industri keuangan dan game:
Layanan broadcast atau data pasar industri keuangan. Misalnya, setelah mendapatkan harga saham dan data real-time lainnya, broker dapat mem-broadcast data saham ke banyak klien secara real time, yang secara efektif mengurangi beban jaringan.
Untuk industri game, broadcast dan multicast terutama digunakan untuk menahan heartbeat di antara beberapa server.

Petunjuk

Mengaktifkan multicast

1. Login ke Konsol VPC.
2. Di daftar VPC, temukan VPC yang diinginkan, dan aktifkan **Multicast** (Multicast).

Menonaktifkan multicast

1. Login ke Konsol VPC.
2. Di daftar VPC, temukan VPC yang diinginkan, dan nonaktifkan **Multicast** (Multicast).

Referensi

Untuk petunjuk selengkapnya mengenai broadcast tingkat subnet, lihat Mengaktifkan atau Menonaktifkan Broadcast.

Menghapus VPC

Waktu update terbaru：2024-01-24 17:48:51

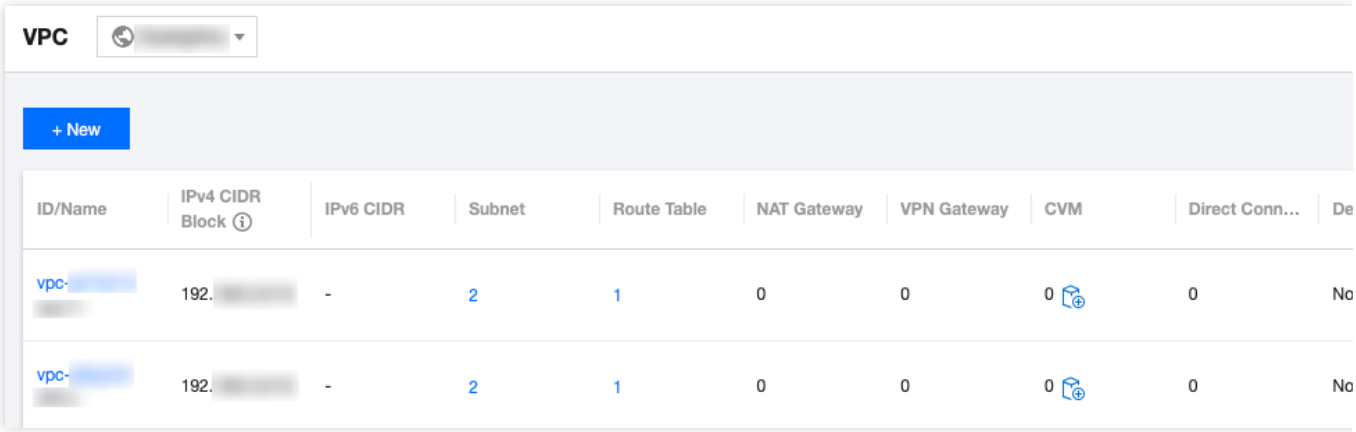
Ketika VPC tidak lagi digunakan dan tidak memiliki sumber daya lain (Peering Connection, ClassicLink, NAT Gateway, VPN Gateway, Direct Connect Gateway, CCN, dan koneksi pribadi) kecuali subnet kosong, tabel perutean, dan ACL jaringan, VPC dapat dihapus.

Keterangan:

Subnet kosong mengacu pada subnet yang tidak menggunakan IP apa pun; yaitu, ketika hanya ada subnet kosong, tabel perutean, dan ACL jaringan di VPC, VPC dapat dihapus; ketika ada penggunaan IP di subnet, VPC tidak dapat dihapus.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas halaman **VPC** (VPC).
3. Dalam daftar VPC, temukan VPC yang akan dihapus, klik **Delete** (Hapus) di bawah kolom **Operation** (Operasi), lalu konfirmasi penghapusan.



Subnet

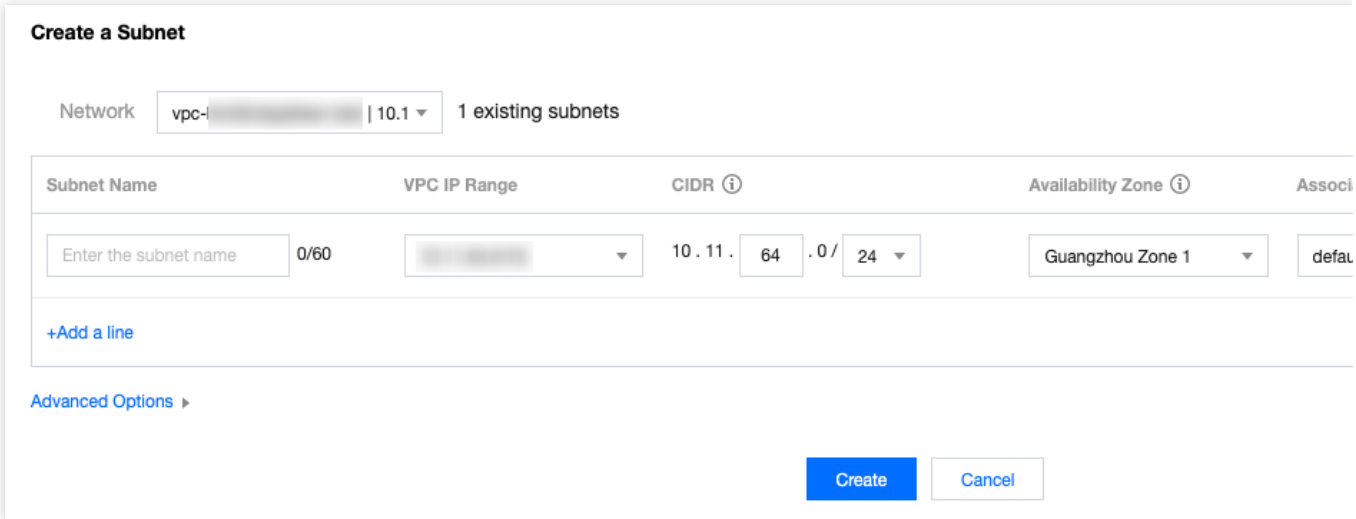
Membuat Subnet

Waktu update terbaru：2024-01-24 17:48:51

Subnet adalah ruang jaringan di VPC, yang membawa semua deployment sumber informasi cloud. VPC memiliki setidaknya satu subnet. Subnet akan dibuat bersama dengan VPC. Anda juga dapat membuat lebih banyak subnet di VPC sesuai dengan kebutuhan bisnis Anda.
Subnet khusus untuk zona ketersediaan. VPC memungkinkan subnet di zona ketersediaan yang berbeda, dan subnet ini dapat berkomunikasi satu sama lain melalui jaringan pribadi secara default. Dokumen ini memandu Anda melalui cara membuat subnet di VPC.

Petunjuk

1. Login ke Konsol VPC.
2. Klik **Subnet** di bilah sisi kiri untuk mengakses halaman pengelolaan.
3. Pilih wilayah dan VPC tempat subnet akan dibuat, lalu klik **+New** (+Baru).
4. Konfigurasikan parameter subnet di kotak dialog pop-up.



Jaringan: VPC tempat subnet berada. VPC yang dipilih di langkah 3 akan ditampilkan secara otomatis. Atau, Anda dapat memilih VPC dari daftar pilihan.
Nama Subnet: masukkan nama subnet kustom dalam 60 karakter.
Rentang IP VPC: blok CIDR dari VPC yang dipilih akan ditampilkan secara otomatis.
CIDR: mengatur blok CIDR dari subnet, yang harus menjadi bagian dari blok CIDR VPC dan tidak boleh tumpang tindih dengan blok CIDR dari subnet lain yang ada di bawah VPC.
Keterangan:

Rencanakan rentang IP subnet yang sesuai dengan skala bisnis Anda. Alamat IP pribadi dalam subnet yang ditentukan akan secara otomatis ditetapkan ke instans CVM yang Anda buat. IP pribadi utama CVM dapat dimodifikasi.Untuk informasi selengkapnya, lihat Memodifikasi IP Pribadi Utama

Zona Ketersediaan: pilih zona ketersediaan tempat subnet berada.

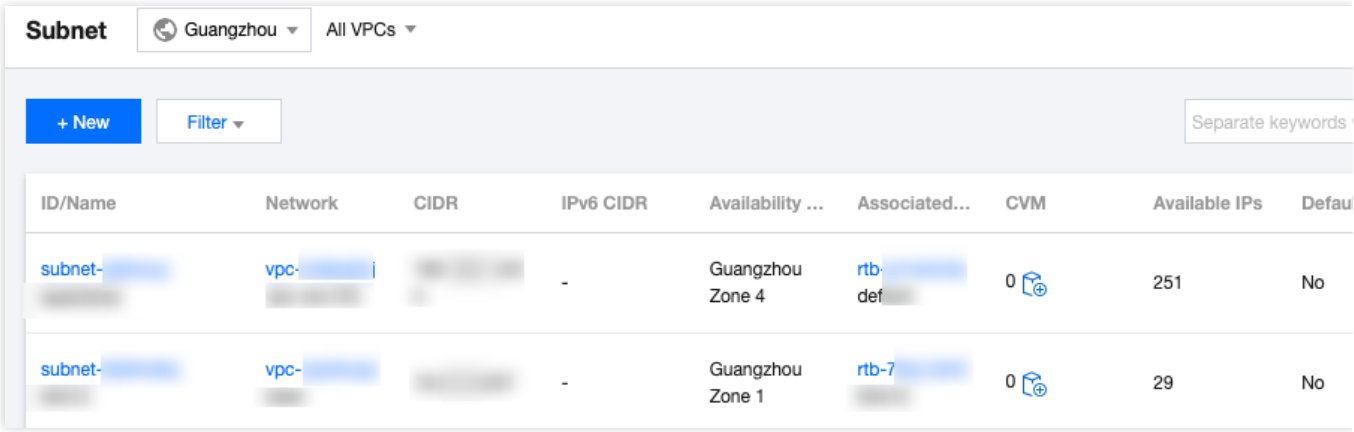
Tabel rute yang terhubung: pilih tabel rute yang akan dihubungkan. Subnet harus dihubungkan dengan tabel rute untuk mengontrol lalu lintas keluar. Tabel rute default VPC akan dihubungkan secara default untuk memastikan interkoneksi jaringan pribadi di VPC. Anda juga dapat memilih tabel rute lain di dalam VPC.

Tambahkan baris: klik **Add a line** (Tambahkan baris) untuk membuat beberapa subnet sekaligus. Klik

untuk menghapus pengaturan subnet yang dipilih.

Opsi Lanjutan: Anda dapat secara opsional mengatur tag untuk subnet agar mengelola sumber informasi subnet dengan lebih baik. Klik **Add** (Tambahkan) untuk mengatur beberapa tag sekaligus. Anda dapat mengeklik ikon di kolom **Operation** (Operasi) untuk menghapus pengaturan tag yang dipilih.

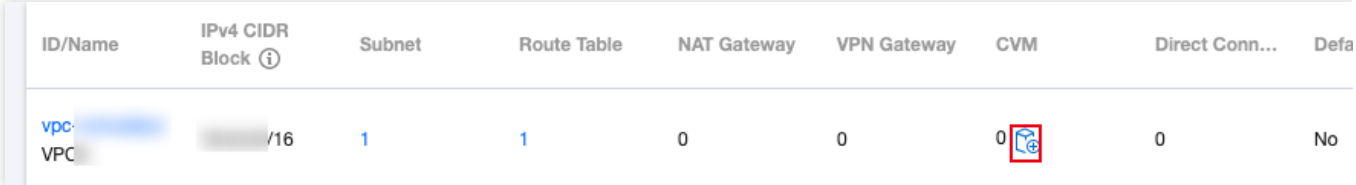
5. Setelah konfigurasi selesai, klik **Create** (Buat). Kemudian subnet yang telah berhasil dibuat akan ditampilkan dalam daftar, seperti ditunjukkan gambar di bawah ini.



Operasi Berikutnya

Setelah membuat subnet, Anda dapat men-deploy sumber informasi termasuk CVM dan CLB di dalamnya.

Klik ikon seperti ditunjukkan gambar di bawah ini untuk langsung membeli CVM di halaman pembelian CVM. Untuk informasi selengkapnya, lihat Membangun VPC IPv4.



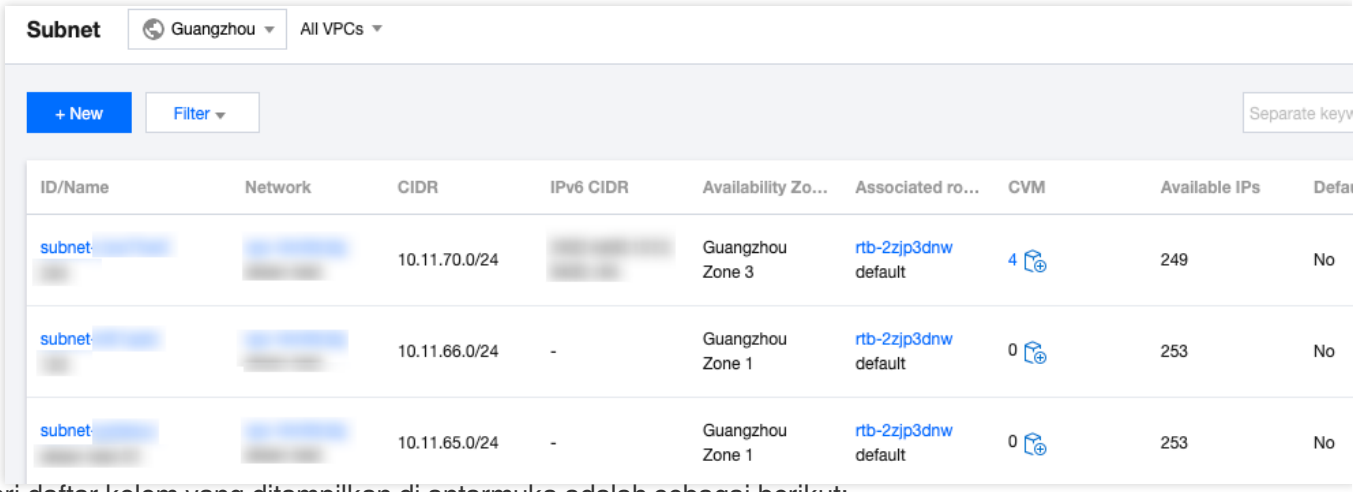
Melihat Subnet

Waktu update terbaru：2024-01-24 17:48:52

Anda dapat melihat sumber informasi semua subnet di VPC di konsol VPC, misalnya, sumber informasi cloud yang di-deploy di subnet, tabel rute yang terhubung dengan subnet, dan aturan ACL yang terikat ke subnet.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih **Subnet** di bilah sisi kiri untuk membuka halaman pengelolaan subnet.
3. Di bagian atas halaman **Subnet**, pilih wilayah dan VPC tempat subnet tersebut berada. Jika Anda mempertahankan nilai default, yaitu **All VPCs** (Semua VPC), Anda dapat melihat semua subnet dari semua VPC di wilayah ini, seperti yang ditampilkan di bawah ini:



Arti dari daftar kolom yang ditampilkan di antarmuka adalah sebagai berikut:

ID/Nama: menampilkan ID dan nama subnet. Setiap subnet diberi ID saat dibuat, dan nama subnet dapat diubah secara real-time.

Jaringan: VPC tempat subnet berada.

CIDR: rentang IP blok CIDR dari subnet. Blok CIDR subnet tidak dapat diubah.

Zona Ketersediaan: menampilkan zona ketersediaan tempat subnet berada.

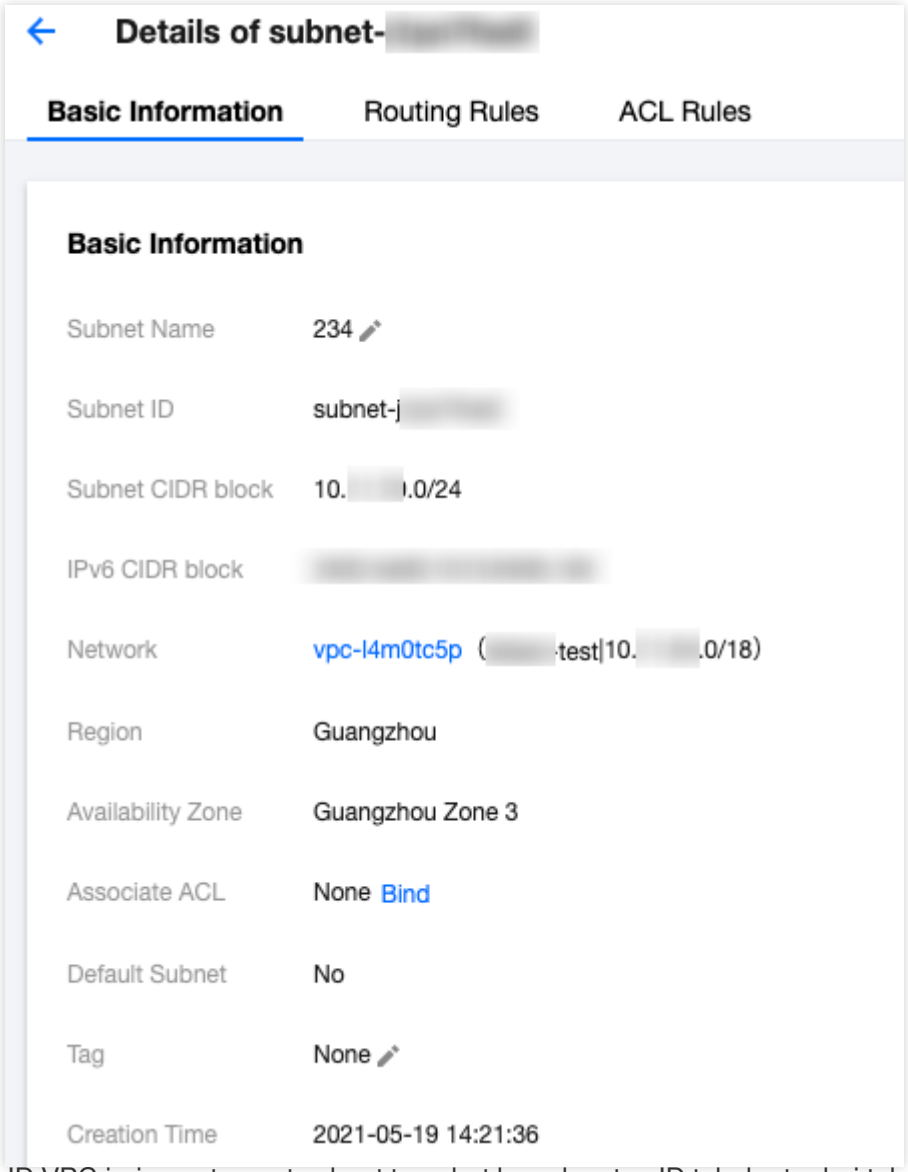
Tabel Rute yang Terhubung: tabel rute yang terhubung dengan subnet.

CVM: menampilkan jumlah CVM yang di-deploy di subnet.

IP yang Tersedia: jumlah alamat IP yang tersedia dalam rentang blok CIDR dari subnet.

Subnet Default: untuk subnet yang dibuat oleh pengguna di halaman **Subnet** di konsol VPC, yang bukan merupakan subnet default, kolom nilai akan menampilkan **No** (Tidak). Jika Anda memilih VPC default dan subnet yang dibuat secara otomatis oleh Tencent Cloud di halaman pembelian CVM, di sini akan muncul **Yes** (Ya). Hanya ada satu VPC dan subnet default di wilayah tertentu.

Waktu Pembuatan: waktu pembuatan subnet.
Operasi: operasi yang dapat dieksekusi untuk subnet. Anda dapat menghapus subnet tanpa sumber informasi, atau Anda dapat mengeklik **More** > **Change Route Table** (Lainnya > Ubah Tabel Rute) untuk mengganti tabel rute yang terhubung dengan subnet.
4. Klik ID subnet untuk melihat detail sumber informasi subnet. Ganti tab untuk melihat aturan perutean dan aturan ACL.



5. Klik ID VPC jaringan tempat subnet tersebut berada, atau ID tabel rute dari tabel rute yang terhubung untuk melihat informasi mendetail tentang sumber informasi terkait.
6. Klik jumlah CVM untuk membuka halaman instans CVM. Jika jumlahnya 0, klik ikon CVM untuk membuka halaman pembelian CVM.
7. Di bagian atas halaman, klik **Filter** untuk melihat daftar subnet di zona ketersediaan yang ditentukan.
8. Klik kotak pencarian di kanan atas halaman untuk membuat kueri dengan cepat berdasarkan **subnet ID**, **Subnet Name**, **Tag**, dan **IPv4 CIDR Block** (ID subnet, Nama Subnet, Tag, dan Blok CIDR IPv4).
9. Klik ikon Pengaturan di kanan atas untuk menyesuaikan kolom yang ditampilkan.

Mengubah Tabel Rute Subnet

Waktu update terbaru：2024-01-24 17:48:51

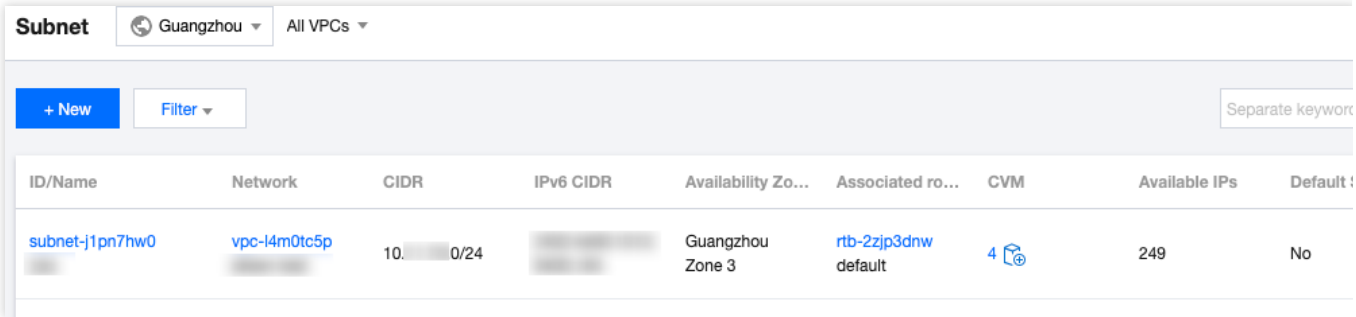
Setiap subnet harus dihubungkan dengan satu tabel rute, yang digunakan untuk mengontrol arah lalu lintas keluar subnet. Anda dapat mengubah tabel rute terkait Subnet di halaman **VPC -> Subnet** sesuai dengan kebutuhan perutean subnet. Jika Anda perlu membuat tabel rute, harap lihat Membuat Tabel Rute Kustom.

Dampak sistem

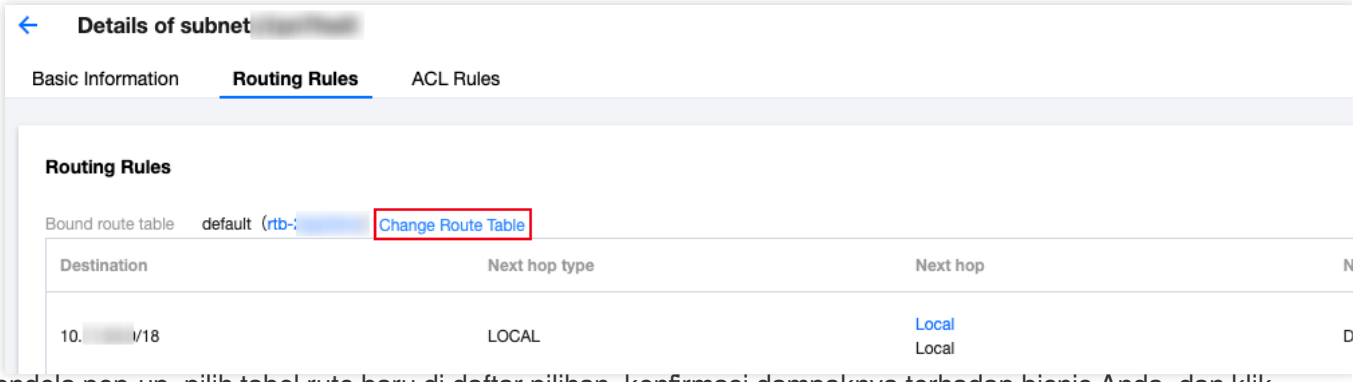
Mempertimbangkan bahwa tabel rute berdampak langsung pada arus lalu lintas di subnet, setiap perubahan seperti hubungan tabel rute atau entri rute harus dipertimbangkan dengan cermat sesuai dengan kebutuhan bisnis aliran jaringan.

Petunjuk

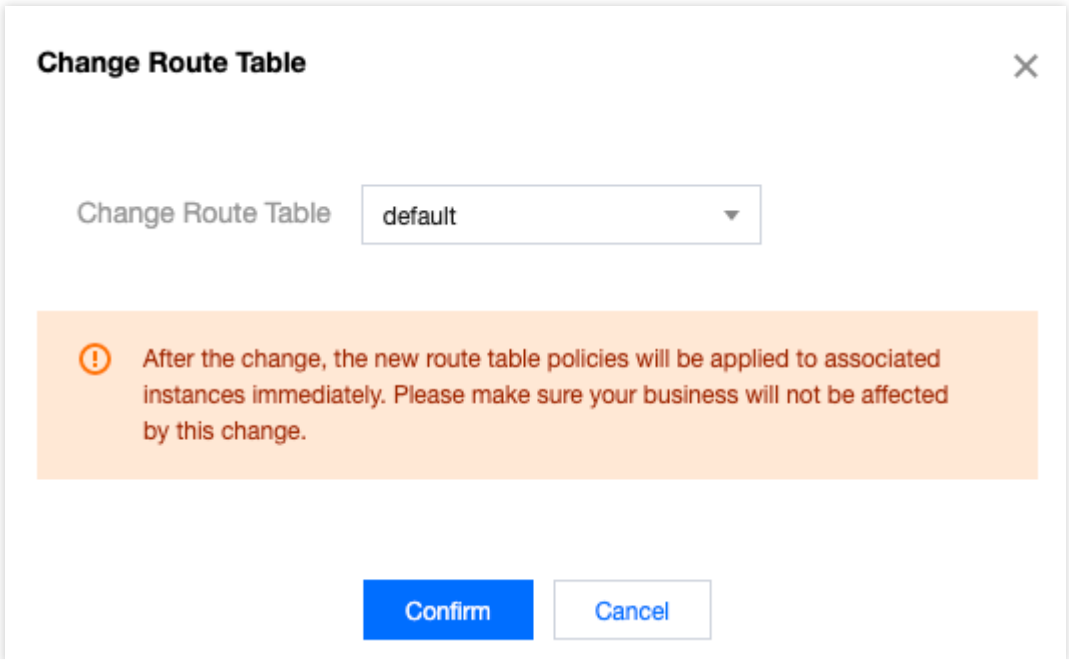
1. Login ke Konsol VPC.
2. Pilih **Subnet** (Subnet) di bilah sisi kiri untuk membuka halaman pengelolaan subnet.
3. Sistem menyediakan dua metode untuk mengubah tabel rute yang terhubung dengan subnet.
Klik **More** > **Change Route Table** (Lainnya > Ubah Tabel Rute) di kolom **Operation** (Operasi) di sisi kanan subnet yang perlu mengubah tabel rute.



Klik ID subnet yang perlu diubah tabel rutenya untuk membuka halaman detail, beralih ke tab **Routing Rules** (Aturan Rute), dan klik **Change Route Table** (Ubah Tabel Rute).



4. Di jendela pop-up, pilih tabel rute baru di daftar pilihan, konfirmasi dampaknya terhadap bisnis Anda, dan klik **Confirm** (Konfirmasi).



Mengelola Aturan ACL

Waktu update terbaru：2024-01-24 17:48:51

Aturan ACL adalah lapisan keamanan opsional yang beroperasi pada tingkat subnet. Ini digunakan untuk mengontrol aliran data masuk dan keluar dari subnet, yang akurat untuk protokol dan granularitas port, untuk mencapai kontrol lalu lintas subnet yang baik. Anda dapat menghubungkan ACL jaringan yang sama ke subnet yang memerlukan tingkat kontrol lalu lintas jaringan yang sama.
Bagian ini menjelaskan cara mengikat, melepaskan, dan mengubah aturan ACL melalui konsol VPC.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih **Subnet** (Subnet) di bilah sisi kiri untuk membuka halaman pengelolaan subnet.
3. Klik ID subnet untuk membuka halaman detailnya. Anda dapat melakukan pengikatan, pelepasan, atau perubahan ACL di halaman berikut.
Di kolom **Associate ACL** (Hubungkan ACL) di bawah tab **Basic Information** (Informasi Dasar)
Di bawah tab **ACL Rules** (Aturan ACL)
4. Lakukan operasi berikut berdasarkan kebutuhan bisnis. Tangkapan layar berikut mengambil operasi di **ACL Rules** (Aturan ACL) sebagai contoh.
Jika subnet saat ini tidak terikat dengan aturan ACL, Anda dapat mengeklik **Bind** (Ikat) untuk memilih aturan ACL yang sesuai, dan klik **OK** (Oke) untuk menyelesaikan pengikatan. Pengikatan akan langsung berlaku. Saat ini, hanya lalu lintas masuk dan keluar dari subnet yang aturannya **Allow** (Izinkan) yang dapat melewatinya.
Jika aturan ACL yang terikat ke subnet saat ini tidak memenuhi persyaratan aliran jaringan, Anda dapat mengeklik **Change** (Ubah) untuk mengubah aturan ACL, yang akan langsung berlaku.
Jika subnet saat ini terikat dengan aturan ACL, tetapi Anda tidak perlu lagi mengontrol lalu lintas masuk dan keluar subnet, Anda dapat mengeklik **Unbind** (Putuskan Ikatan) untuk memutuskan ikatan aturan ACL. Pemutusan ikatan akan langsung berlaku dan ini akan menyebabkan pencabutan pembatasan aturan ACL pada lalu lintas masuk dan keluar subnet.

Mengaktifkan atau Menonaktifkan Broadcast

Waktu update terbaru：2024-01-24 17:48:51

Latar belakang

Multicast dan broadcast adalah mode komunikasi satu ke semuanya, yang dapat membantu perusahaan mengurangi konsumsi bandwidth jaringan dan beban jaringan melalui transmisi data efisien point-to-multipoint.
Dalam mode unicast, server yang memulai mengirimkan data ke N server secara terpisah. Jika multicast digunakan, server mengirimkan data yang sama ke N server hanya sekali, yang mengurangi konsumsi sumber informasi server serta sumber informasi bandwidth jaringan backbone.
Multicast: Tencent Cloud mendukung multicast pada dimensi VPC.
Broadcast: Tencent Cloud mendukung broadcast pada dimensi subnet.
Keterangan:
Fitur broadcast dan multicast saat ini dalam uji beta. Jika diperlukan, harap kirim tiket.
Saat ini wilayah yang mendukung multicast dan broadcast adalah: Beijing, Shanghai, Guangzhou, Chengdu, Chongqing, Nanjing, Hong Kong (Tiongkok), Singapura, Seoul, Tokyo, Bangkok, Toronto, Silicon Valley, Virginia, Frankfurt, dan Moscow.

Ikhtisar

Multicast dan broadcast sebagian besar digunakan dalam industri keuangan dan game:
Layanan broadcast atau data pasar industri keuangan. Misalnya, setelah mendapatkan harga saham dan data real-time lainnya, broker dapat mem-broadcast data saham ke banyak klien secara real time, yang secara efektif mengurangi beban jaringan.
Untuk industri game, broadcast dan multicast terutama digunakan untuk menahan heartbeat di antara beberapa server.
Dokumen ini menjelaskan cara mengaktifkan atau menonaktifkan broadcast untuk subnet.

Petunjuk

Mengaktifkan broadcast

1. Login ke Konsol VPC.
2. Klik **Subnet** (Subnet) di bilah sisi kiri untuk mengakses halaman admin.

3. Dalam daftar VPC, cari VPC target, dan alihkan tombol ke **Enable** (Aktifkan) di bawah kolom **Subnet broadcast** (Broadcast subnet).

Menonaktifkan broadcast

1. Login ke Konsol VPC.
2. Klik **Subnet** (Subnet) di bilah sisi kiri untuk mengakses halaman admin.
3. Dalam daftar VPC, cari VPC target, dan alihkan tombol ke **Disable** (Nonaktifkan) di bawah kolom **Subnet broadcast** (Broadcast subnet).

Referensi

Untuk informasi selengkapnya mengenai multicast tingkat VPC, lihat Mengaktifkan atau Menonaktifkan Multicast.

Menghapus Subnet

Waktu update terbaru：2024-01-24 17:48:51

Anda dapat menghapus subnet yang tidak lagi digunakan dan tidak menggunakan sumber daya IP apa pun.

Keterangan:

Saat ini, sumber daya Tencent Cloud yang melibatkan penggunaan IP dalam subnet termasuk CVM, jaringan pribadi CLB, ENI, HAVIP, SCF, TKE, dan TencentDB (untuk MySQL, Redis, TDSQL, dll.).

Petunjuk

1. Login ke Konsol VPC.
2. Klik **Subnet** (Subnet) di bilah sisi kiri untuk mengakses halaman pengelolaan.
3. Di bagian atas daftar, pilih wilayah dan VPC tempat subnet yang akan dihapus.
4. Dalam daftar, pilih subnet yang akan dihapus, klik **Delete** (Hapus) di kolom **Operation** (Operasi), dan klik **OK** (OKE).

Tabel Rute

Ikhtisar

Waktu update terbaru：2024-01-24 17:48:51

Tabel rute terdiri dari beberapa kebijakan perutean yang mengontrol arah lalu lintas keluar dari subnet di VPC. Setiap subnet hanya dapat dihubungkan dengan satu tabel rute, sedangkan setiap tabel rute dapat dihubungkan dengan beberapa subnet. Anda dapat membuat beberapa tabel rute untuk subnet dengan rute lalu lintas yang berbeda.

Jenis

Ada dua jenis tabel rute: default dan kustom.
Default route table (Tabel rute default): saat Anda membuat VPC, sistem secara otomatis menghasilkan tabel rute default yang akan dihubungkan ke subnet yang dibuat nanti jika tidak ada tabel rute kustom yang dipilih. Anda tidak dapat menghapus tabel rute default, tetapi dapat menambahkan, menghapus, dan mengubah kebijakan perutean di dalamnya.
Custom route table (Tabel rute kustom): Anda dapat membuat atau menghapus tabel rute kustom di VPC. Tabel rute kustom ini dapat dihubungkan ke semua subnet untuk menerapkan kebijakan perutean yang sama.
Keterangan:
Anda dapat menghubungkan tabel rute saat membuat subnet, atau mengubah tabel rute setelah subnet dibuat.

Kebijakan Perutean

Tabel rute mengontrol rute lalu lintas dengan menggunakan kebijakan perutean. Kebijakan perutean terdiri dari tujuan, jenis hop selanjutnya, dan hop selanjutnya.
Destination (Tujuan): menentukan rentang IP tujuan yang Anda inginkan untuk meneruskan lalu lintas. Tujuan harus berupa rentang IP. Jika Anda ingin memasukkan satu alamat IP, atur mask ke `32` (misalnya, `172.16.1.1/32`). Tujuan tidak boleh berupa rentang IP untuk VPC tempat tabel rute, karena rute lokal telah mengizinkan interkoneksi jaringan pribadi di VPC ini.
Keterangan:
Jika Anda telah men-deploy layanan TKE di VPC, tujuan yang Anda konfigurasikan dalam kebijakan perutean subnet VPC tidak boleh berada dalam blok CIDR VPC atau berisi rentang IP TKE.
Misalnya, jika blok CIDR VPC adalah `172.168.0.0/16` dan blok TKE CIDR adalah `192.168.0.0/16`, rentang IP tujuan tidak boleh berada dalam `172.168.0.0/16`, atau berisi `192.168 .0.0/16` saat Anda mengonfigurasi kebijakan perutean untuk subnet VPC.

Next-hop type (Jenis hop selanjutnya): menunjukkan jalan keluar paket data untuk VPC. Jenis VPC hop selanjutnya mendukung **NAT Gateway** (NAT Gateway), **Peering connection** (Peering connection), **VPN gateway** (VPN gateway), **Direct connect gateway** (Direct connect gateway), **CVM** (CVM), dan lainnya.
Next hop (Hop selanjutnya): menentukan instans hop selanjutnya (diidentifikasi dengan ID hop selanjutnya) yang menjadi tujuan penerusan lalu lintas, seperti NAT Gateway di VPC.

Prioritas kebijakan perutean

Ketika ada beberapa kebijakan perutean dalam tabel rute, prioritas perutean berikut berlaku, dari tinggi ke rendah:
Lalu lintas dalam VPC: lalu lintas dalam VPC dicocokkan terlebih dahulu.
Rute yang sama persis (pencocokan awalan terpanjang): ketika ada beberapa rute di tabel rute yang dapat cocok dengan IP tujuan, rute dengan mask terpanjang (persis) dicocokkan untuk menentukan hop selanjutnya.
IP Publik: jika tidak ada kebijakan perutean yang cocok, instans CVM dapat mengakses internet melalui alamat IP publiknya.
Use case: (Kasus penggunaan:)
Ketika subnet dihubungkan ke NAT Gateway, dan CVM di subnet memiliki IP publik (atau EIP), CVM mengakses internet melalui NAT Gateway secara default (karena prioritas rute yang sama persis lebih tinggi dari prioritas IP publik). Namun, Anda dapat mengatur kebijakan perutean untuk mengizinkan CVM mengakses internet menggunakan alamat IP publiknya. Untuk informasi detailnya, lihat Menyesuaikan Prioritas NAT Gateway dan EIP.

ECMP

Equal-cost Multipath Routing (ECMP) berarti ada beberapa rute dengan biaya yang sama ke satu tujuan. Teknologi perutean tradisional hanya menggunakan satu jalur untuk mentransfer paket ke tujuan yang sama, sedangkan jalur yang tersisa dalam status siaga atau tidak valid. Ketika jalur gagal, perlu waktu untuk menggunakan jalur lain. Sebaliknya, ECMP menggunakan beberapa rute dengan biaya yang sama di lingkungan jaringan untuk meningkatkan bandwidth transmisi, menyeimbangkan lalu lintas melalui beberapa rute, dan mencapai pencadangan dengan tautan yang berlebihan.
VPC mendukung ECMP untuk jenis rute yang sama, seperti yang dijelaskan secara mendetail di bawah ini.

Jenis hop selanjutnya	Mendukung ECMP (jenis rute yang sama)	Jumlah maksimum ECMP
NAT Gateway	Tidak	T/A
IP publik CVM	Tidak	T/A
CVM	Ya	8
Peering connection	Tidak	T/A
Direct connect gateway	Ya	8

CCN	Tidak	T/A
HAVIP	Ya	8
VPN gateway	Ya	8

Keterangan:

CCN mendukung satu ECMP dengan direct connect gateway atau peering connection.

Kasus penggunaan

ECMP sering digunakan untuk menyeimbangkan beban lalu lintas melalui gateway dengan bandwidth terbatas. Asumsikan Anda memerlukan 2000 Mbps untuk menghubungkan bisnis berbasis VPC dan IDC Anda, tetapi bandwidth VPN maksimum saat ini adalah 1000 Mbps. Untuk mencapai tujuan, Anda dapat membuat dua VPN gateway 1000-Mbps dan dua tunnel VPN.

Rute Primer/Sekunder

Rute primer/sekunder mengacu pada dua jalur atau lebih ke tujuan yang sama, dengan satu jalur aktif dan jalur siaga atau tidak valid. Asumsikan bahwa ada dua rute VPC ke IDC, yaitu jalur A dan jalur B. Semua paket dikirim ke tujuan melalui jalur A, sedangkan jalur B tidak valid atau siaga. Saat jalur A mengalami kegagalan penautan, Anda dapat mengaktifkan jalur B untuk mengambil alih lalu lintas dari jalur A, sehingga memastikan ketersediaan aplikasi. Dalam hal ini, jalur A dan B disebut rute primer dan sekunder.

Jenis hop selanjutnya menentukan prioritas rute. Saat menambahkan kebijakan perutean ke tabel rute VPC, Anda dapat mengonfigurasi berbagai jenis gateway untuk bertindak sebagai rute primer dan sekunder ke satu tujuan. Kemudian, pemeriksaan jaringan VPC dapat digunakan untuk memeriksa kualitas penautan dan aksesibilitas. Setelah mengonfigurasi kebijakan alarm, Anda dapat segera mendeteksi pengecualian penautan apa pun dan beralih antara rute primer dan sekunder dengan cepat untuk memenuhi persyaratan ketersediaan tinggi.

Keterangan:

Fitur prioritas rute saat ini dalam versi beta. Untuk menggunakannya, harap kirim tiket.

Jenis hop selanjutnya menentukan prioritas rute di tabel rute VPC. Secara default, prioritas rute dari tingkat tinggi ke rendah adalah CCN, direct connect gateway, VPN gateway, dan lainnya.

Saat ini, Anda tidak dapat menyesuaikan prioritas rute di konsol. Jika diperlukan, harap kirim tiket.

Tabel berikut menjelaskan dukungan primer/sekunder dari berbagai jenis rute VPC.

Jenis hop selanjutnya	Dukungan untuk rute primer/sekunder
NAT Gateway	Tidak
IP publik CVM	Tidak

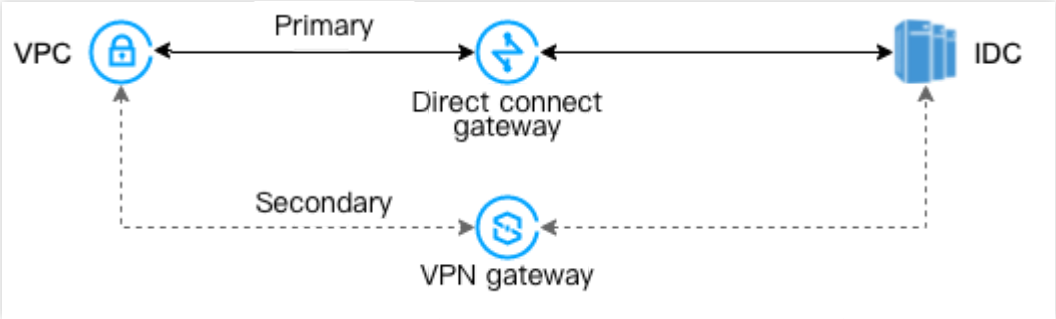
CVM	Ya, dengan CCN, VPN gateway, direct connect gateway, atau HAVIP
Peering connection (dalam wilayah)	Tidak
Peering connection (lintas wilayah)	Tidak
Direct connect gateway	Ya, dengan CCN, VPN gateway, HAVIP, atau CVM
CCN	Ya, dengan VPN gateway, direct connect gateway, HAVIP, atau CVM
HAVIP	Ya, dengan CCN, VPN gateway, direct connect gateway, atau CVM
VPN gateway	Ya, dengan CCN, direct connect gateway, HAVIP, atau CVM

Kasus penggunaan

Rute primer/sekunder sering digunakan untuk meneruskan lalu lintas dengan lancar saat penautan gateway gagal.

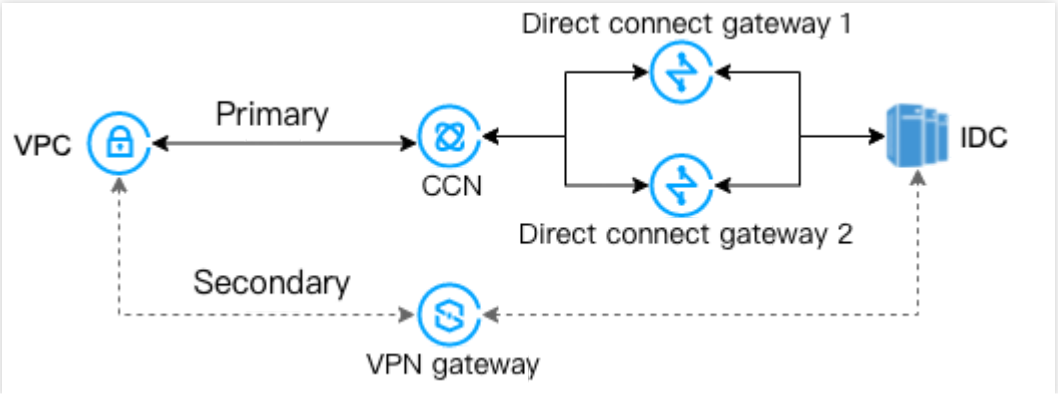
Direct connect gateway (primer) berbasis VPC dan VPN gateway untuk VPC (sekunder)

Scenario (Skenario): interkoneksikan Tencent Cloud VPC dan IDC lokal melalui direct connect gateway berbasis VPC. Sementara itu, buat tunnel VPN melalui VPN gateway untuk bertindak sebagai penautan komunikasi sekunder antara IDC dan VPC.



Direct connect gateway (primer) berbasis CCN dan VPN gateway untuk VPC (sekunder)

Scenario (Skenario): interkoneksikan Tencent Cloud VPC dan IDC lokal melalui instans CCN. Sementara itu, buat tunnel VPN melalui VPN gateway untuk bertindak sebagai penautan komunikasi sekunder antara IDC dan VPC.



Keterangan

Waktu update terbaru：2024-01-24 17:48:51

Tabel rute default VPC tidak dapat dihapus.
Setelah VPC dibuat, tabel rutenya akan otomatis disediakan dengan rute default yang menunjukkan bahwa semua sumber daya di VPC ini saling terhubung melalui jaringan pribadi. Kebijakan perutean ini tidak dapat diubah atau dihapus.

Tujuan	Jenis hop selanjutnya	Hop selanjutnya
Lokal	Lokal	Lokal

Protokol perutean dinamis seperti BGP dan OSPF tidak didukung.
Rute dapat dipublikasikan ke CCN. Rute berikut dapat dipublikasikan ke CCN.

Jenis hop selanjutnya	Menerbitkan ke CCN secara default	Penerbitan atau penarikan secara manual	Deskripsi
Lokal	Didukung	Tidak Didukung	Ditetapkan oleh sistem. Rentang IP VPC yang terhubung ke CCN akan otomatis dipublikasikan ke CCN, termasuk blok CIDR utama dan sekunder (kecuali untuk rentang IP TKE).
CVM	Tidak Didukung	Didukung	Rute kustom ke CVM. Jika rentang IP semuanya 0 atau kebijakan perutean dinonaktifkan, rute tidak dapat dipublikasikan ke CCN.
HAVIP	Tidak Didukung	Didukung	Rute kustom ke HAVIP. Jika rentang IP semuanya 0 atau kebijakan perutean dinonaktifkan, rute tidak dapat dipublikasikan ke CCN.

Keterangan:
Rute kustom yang dinonaktifkan tidak dapat dipublikasikan ke CCN.
Rute kustom harus ditarik terlebih dahulu sebelum dapat dinonaktifkan jika telah dipublikasikan ke CCN.

Batasan Kuota

Sumber daya	Batas

Jumlah tabel rute per VPC	10
Jumlah tabel rute yang terhubung ke setiap subnet	1
Jumlah kebijakan perutean per tabel rute	50

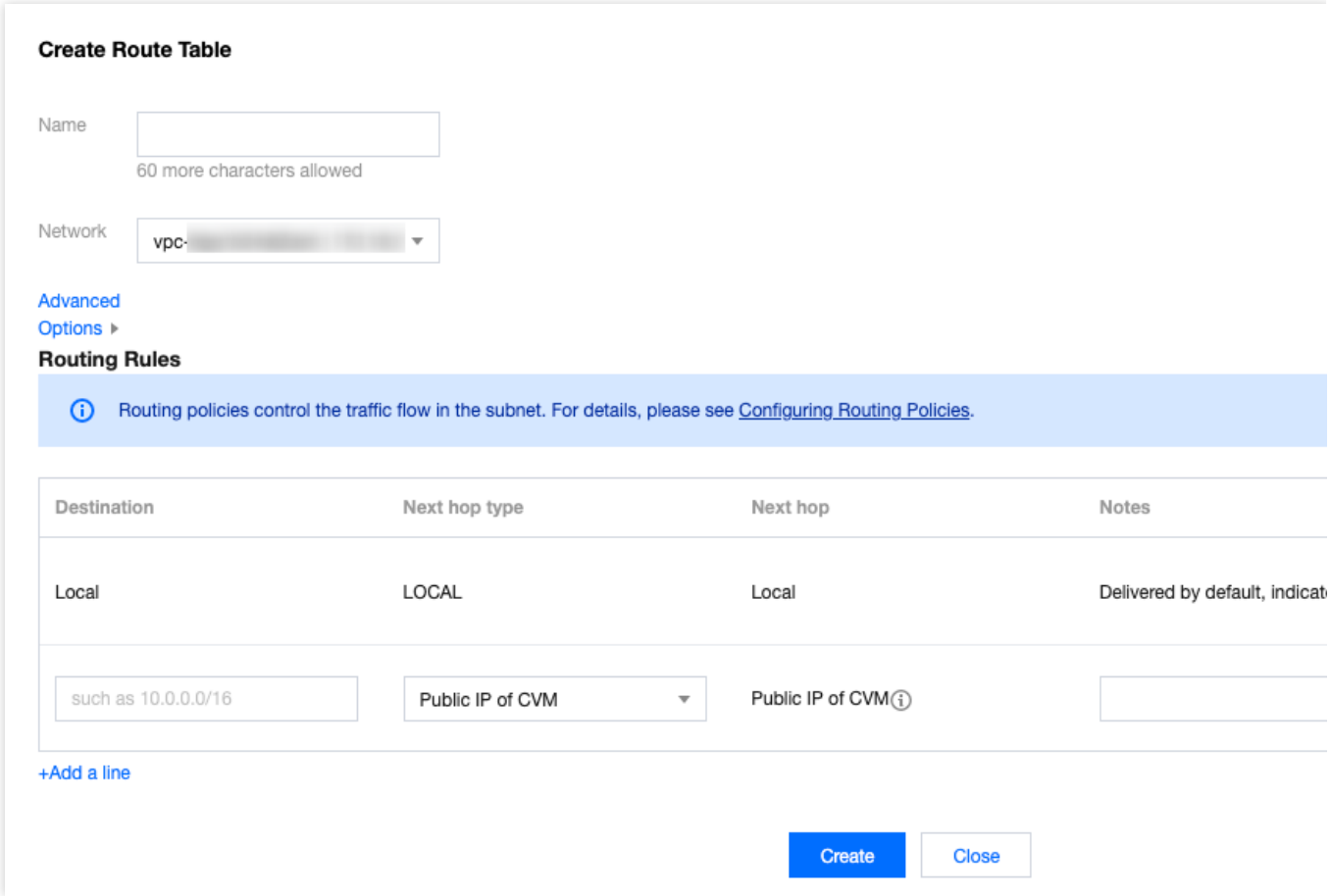
Membuat Tabel Rute Kustom

Waktu update terbaru：2024-01-24 17:48:51

Tabel rute digunakan untuk mengontrol lalu lintas keluar dari subnet. Ini dapat berisi beberapa kebijakan perutean yakni, tabel rute default dan tabel rute kustom. Tabel rute default (rute lokal) memungkinkan interkoneksi jaringan pribadi di VPC, yang tidak dapat dihapus, tetapi dapat dikonfigurasi dengan kebijakan perutean dengan cara yang sama saat Anda mengonfigurasi tabel rute kustom. Dokumen ini menjelaskan cara membuat dan mengonfigurasi tabel rute kustom.

Petunjuk

1. Login ke Konsol VPC.
2. Klik **Route Tables** (Tabel Rute) di bilah sisi kiri untuk mengakses halaman pengelolaan.
3. Klik **+ New** (+ Baru).
4. Pada dialog pop-up, masukkan nama tabel rute, pilih VPC tempat tabel rute, dan konfigurasi kebijakan perutean.



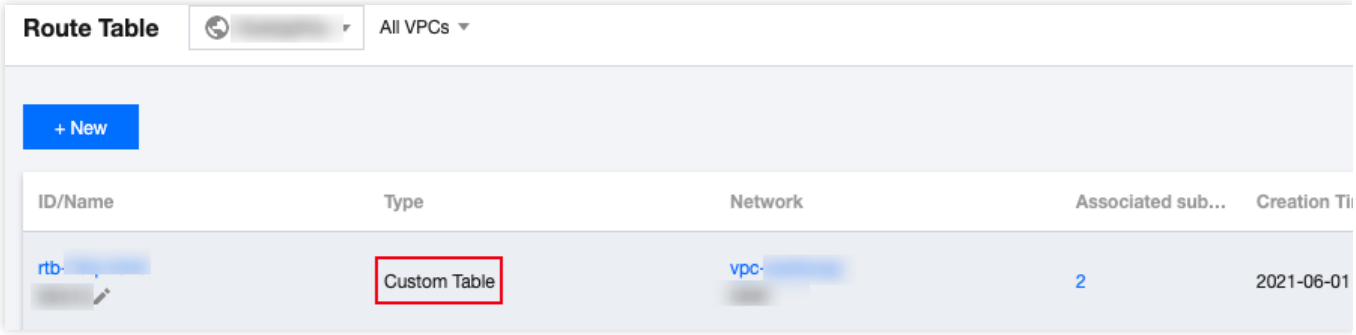
Keterangan:

Anda dapat mengonfigurasi kebijakan perutean saat membuat tabel rute. Atau, setelah tabel rute dibuat, Anda dapat mengeklik ID tabel rute untuk masuk ke halaman **Basic Information** (Informasi Dasar) dan klik **+ New routing policies** (+ Kebijakan perutean baru) untuk mengonfigurasi kebijakan perutean.

Mengonfigurasi kebijakan perutean :

Parameter	Deskripsi
Tujuan	Rentang IP tujuan tempat lalu lintas diteruskan. Konfigurasi harus memenuhi persyaratan berikut: Masukkan rentang IP. Jika Anda ingin memasukkan satu IP, atur mask ke 32 (misalnya, `172.16.1.1/32`). Tujuan tidak boleh berupa rentang IP VPC tempat tabel rute berada karena rute lokal telah mengizinkan interkoneksi jaringan pribadi di VPC ini. **Catatan**: Jika telah men-deploy Layanan TKE di VPC, tujuan yang Anda konfigurasikan di kebijakan tabel rute subnet VPC tidak boleh berada dalam blok CIDR VPC atau berisi rentang IP TKE. Misalnya, jika blok CIDR VPC adalah `172.168.0.0/16` dan blok TKE CIDR adalah `192.168.0.0/16`, rentang IP tujuan tidak boleh berada dalam `172.168.0.0/16`, atau berisi `192.168 .0.0/16` saat Anda mengonfigurasi kebijakan perutean untuk subnet VPC.
Jenis hop selanjutnya	Jalur keluar dari paket data VPC. Berikut adalah jenis yang didukung: NAT Gateway: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke NAT Gateway. Peering Connections: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke VPC di sisi lain koneksi peering. Direct Connect Gateway: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke direct connect gateway. IP Virtual Ketersediaan Tinggi: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke HAVIP. VPN Gateway: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke VPN gateway. IP publik CVM: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke IP publik (termasuk EIP) instans CVM di VPC. CVM: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke instans CVM di VPC.
Hop selanjutnya	Menentukan instans hop selanjutnya yang menjadi tujuan pengalihan lalu lintas, seperti gateway atau IP CVM.
Catatan	Menjelaskan tujuan rute untuk pengelolaan sumber daya. Parameter ini bersifat opsional.
Tambahkan baris	mengonfigurasi beberapa kebijakan perutean jika diperlukan. Anda dapat mengeklik ikon penghapusan di kolom **Operation** (Operasi) untuk menghapus kebijakan perutean yang tidak perlu. Tabel rute kustom setidaknya harus berisi satu kebijakan perutean.

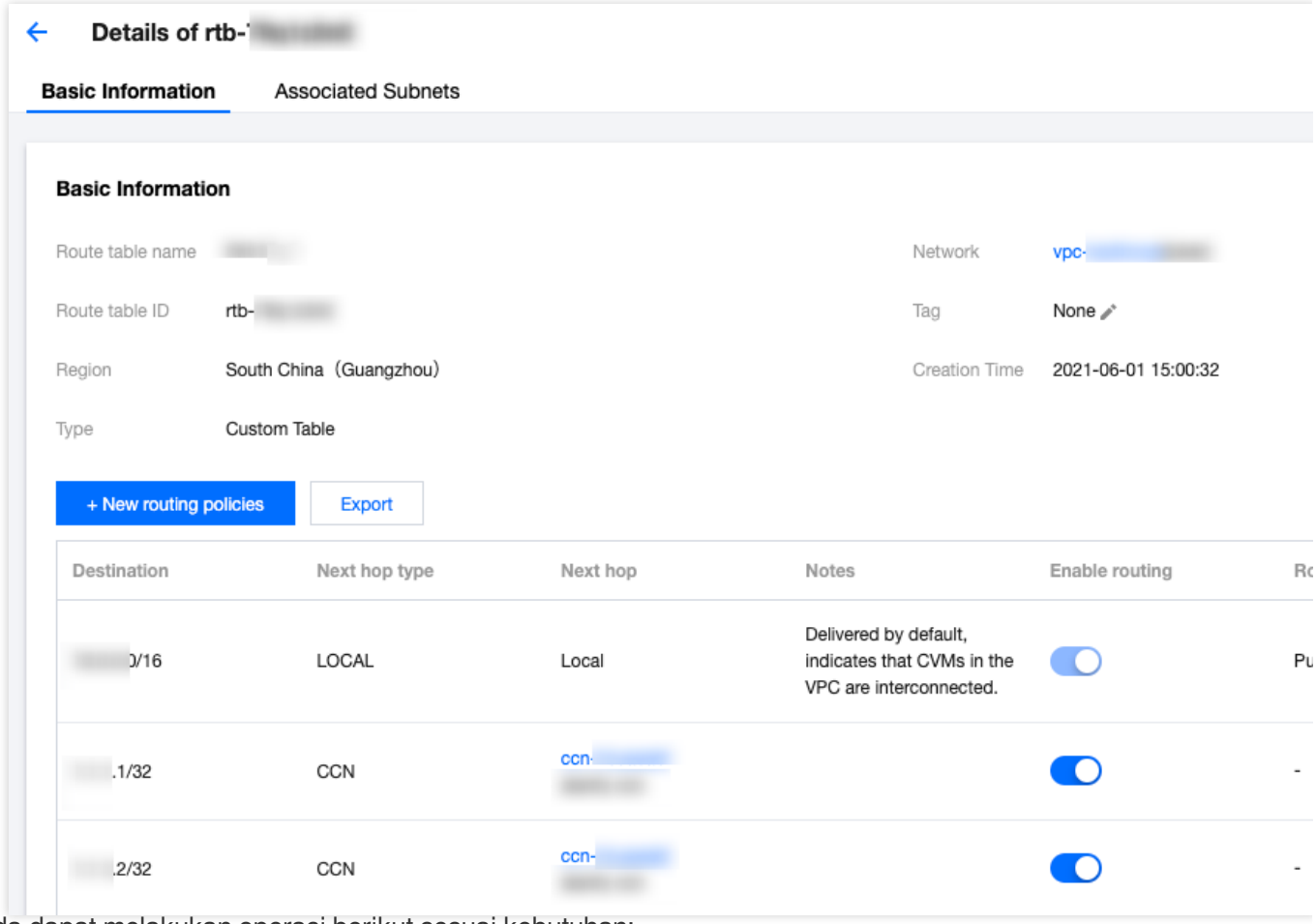
5. Setelah konfigurasi selesai, klik **Create** (Buat). Kemudian tabel rute akan ditampilkan dalam daftar.



Mengonfigurasi HAVIP

Saat ini, hanya kebijakan perutean dengan **Next hop type** (Jenis hop selanjutnya) yang memiliki **High Availability Virtual IP** (IP Virtual Ketersediaan Tinggi), **VPN Gateway**, atau **CVM** dalam tabel rute default atau kustom yang dapat dipublikasikan secara manual ke atau ditarik dari CCN.

1. Klik ID tabel rute untuk masuk ke halaman detail.



2. Anda dapat melakukan operasi berikut sesuai kebutuhan:

Klik **Publish to CCN** (Publikasikan ke CCN) untuk memublikasikan kebijakan perutean yang diaktifkan ke CCN.

Klik **Withdraw from CCN** (Tarik dari CCN) untuk menarik kebijakan perutean kustom yang telah dipublikasikan ke CCN.

Klik **Edit** (Edit) untuk mengubah kebijakan perutean.

Klik **Delete** (Hapus) untuk menghapus kebijakan perutean yang dinonaktifkan.

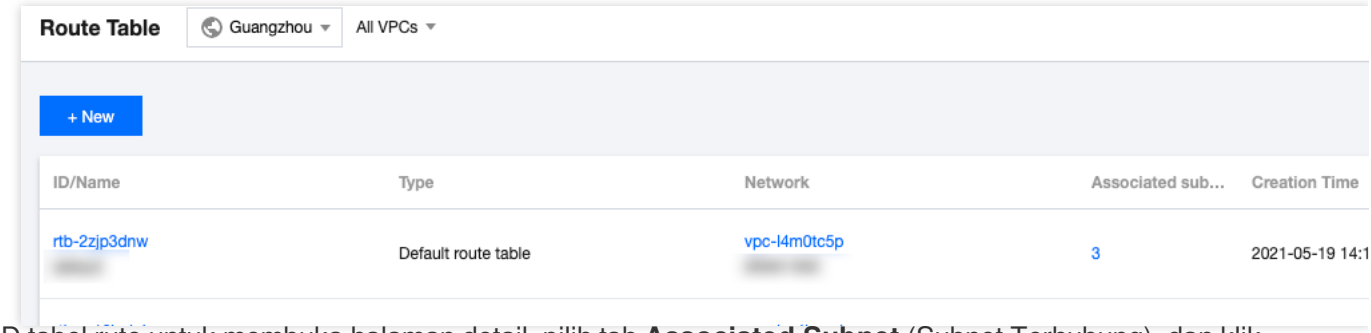
Menghubungkan atau Memutuskan Hubungan Subnet

Waktu update terbaru：2024-01-24 17:48:51

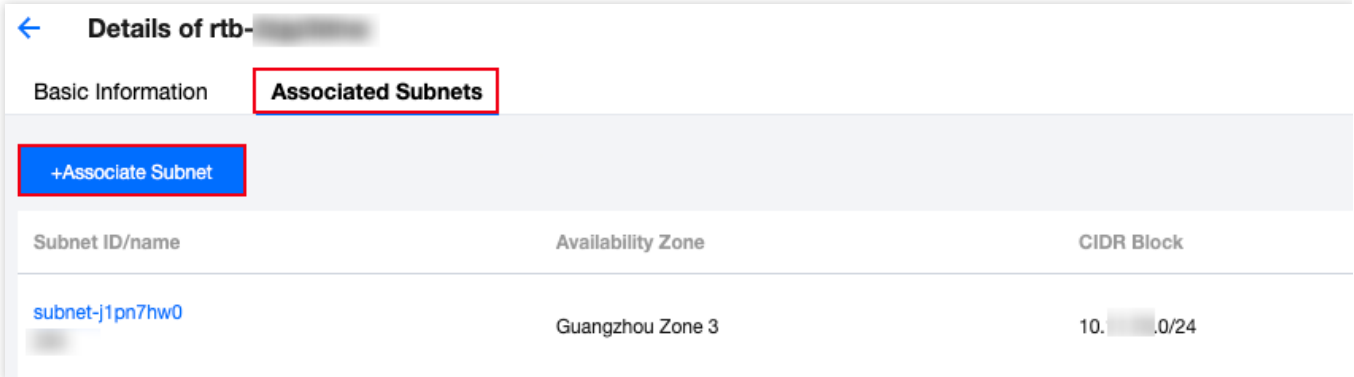
Setelah dibuat, tabel rute perlu dihubungkan ke subnet untuk mengontrol lalu lintas keluar dari subnet. Dokumen ini menjelaskan cara menghubungkan tabel rute dengan atau memisahkannya dari subnet.

Menghubungkan ke Subnet

1. Login ke Konsol VPC.
2. Pilih **Rute Tables** (Tabel Rute) di bilah sisi kiri untuk membuka halaman pengelolaan.
3. Ada dua metode untuk menghubungkan ke subnet:
Dalam daftar, pilih tabel rute yang perlu dihubungkan ke subnet, dan klik **More** (Lainnya)> **Associated Subnet** (Subnet Terhubung) di kolom **Operation** (Operasi).



Klik ID tabel rute untuk membuka halaman detail, pilih tab **Associated Subnet** (Subnet Terhubung), dan klik **+Associate Subnet** (+Hubungkan Subnet).



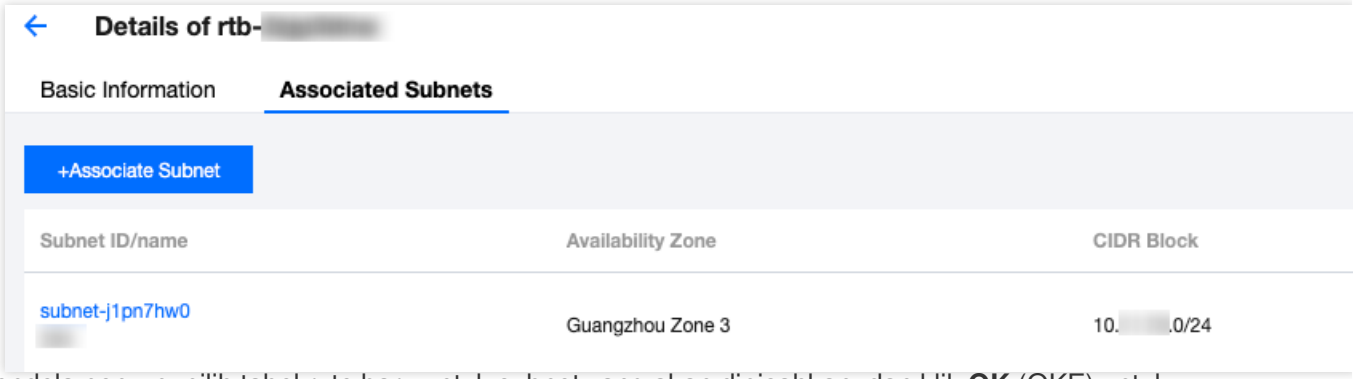
4. Di jendela pop-up, pilih subnet yang akan dihubungkan (tabel rute dapat dihubungkan ke beberapa subnet secara bersamaan, dan Anda dapat memfilter menurut ID/nama subnet dengan cepat). Harap evaluasi dampak bisnis dari koneksi ke subnet. Konfirmasi dampaknya, dan klik **OK** (OKE).

Perhatian:

Setelah tabel rute dihubungkan ke subnet, tabel rute asli yang terhubung ke subnet akan diganti dengan yang baru, dan lalu lintas keluar subnet akan dijalankan sesuai dengan kebijakan di tabel rute baru. Harap evaluasi dampak bisnis dengan cermat.

Pemutusan Koneksi dari Subnet

1. Login ke Konsol VPC.
2. Pilih **Rute Tables** (Tabel Rute) di bilah sisi kiri untuk membuka halaman pengelolaan.
3. Klik ID tabel rute untuk membuka halaman detail, beralih ke tab **Associated Subnet** (Subnet Terhubung), dan klik **Disassociate** (Putuskan Koneksi).



4. Di jendela pop-up, pilih tabel rute baru untuk subnet yang akan dipisahkan, dan klik **OK** (OKE) untuk menyelesaikan pemutusan koneksi tabel rute saat ini dari subnet. Kebijakan lalu lintas keluar subnet akan dijalankan berdasarkan tabel rute baru yang dipilih untuknya.

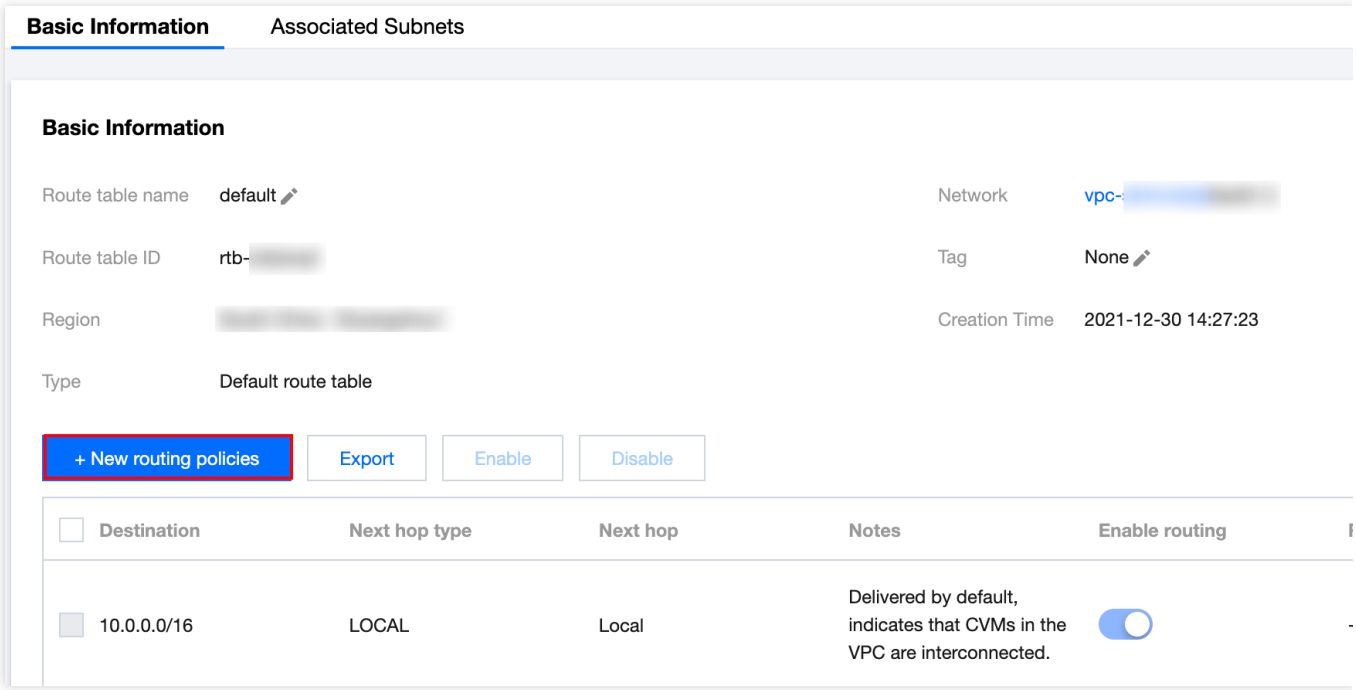
Mengelola Kebijakan Perutean

Waktu update terbaru：2024-01-24 17:48:51

Dokumen ini menjelaskan operasi yang terkait dengan kebijakan perutean.

Menambahkan Kebijakan Perutean

1. Login ke konsol VPC, dan akses halaman **Route Table** (Tabel Rute).
2. Klik **ID/Name** (ID/Nama) dari tabel rute yang akan dimodifikasi untuk membuka halaman detailnya.
3. Klik **+New routing policies** (+Kebijakan perutean baru).



4. Pada je

ndela p

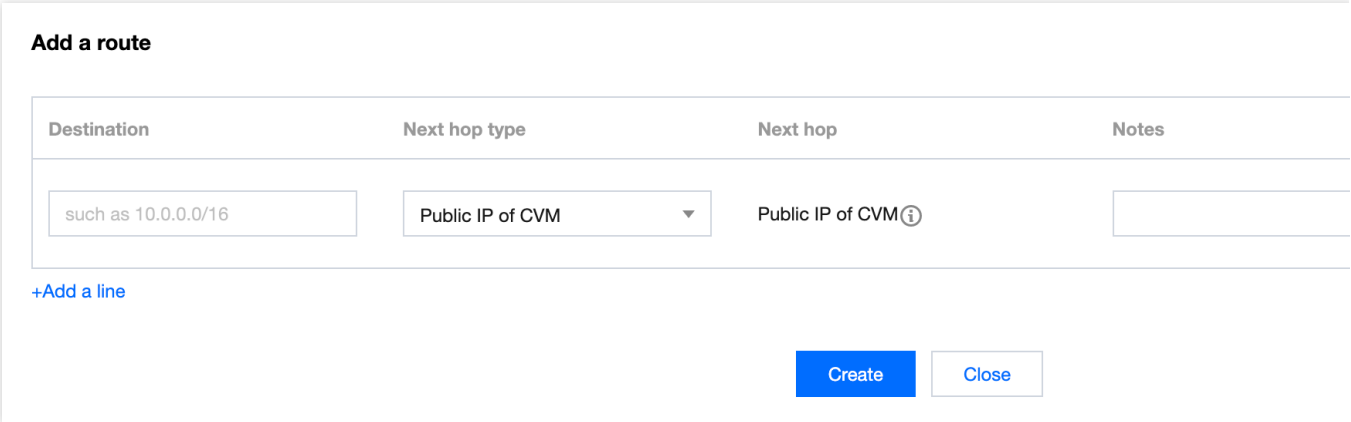
op-up, konfigurasikan kebijakan perutean.

Keterangan:

Jika Anda telah men-deploy layanan TKE di VPC, tujuan yang Anda konfigurasikan dalam kebijakan perutean subnet VPC tidak boleh tumpang tindih dengan blok CIDR VPC atau rentang IP TKE. >Misalnya, jika blok CIDR VPC adalah `172.168.0.0/16` dan blok TKE CIDR adalah `192.168.0.0/16` , rentang IP tujuan tidak boleh berada dalam `172.168.0.0/16` , atau berisi `192.168 .0.0/16` .

Item Konfigurasi	Deskripsi

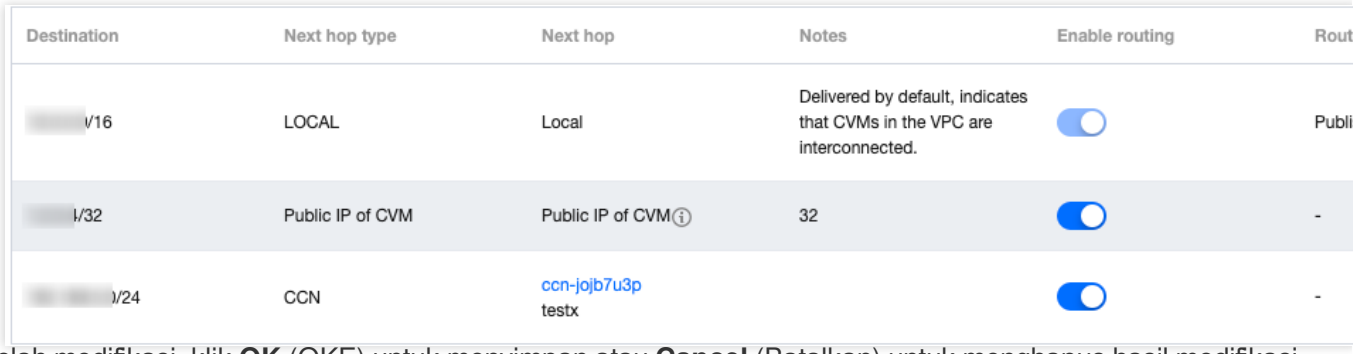
Tujuan	Menentukan rentang IP tujuan tempat Anda ingin meneruskan lalu lintas keluar subnet. Persyaratan untuk tujuan adalah sebagai berikut: Masukkan rentang IP. Jika Anda ingin memasukkan satu IP, atur mask ke `32` (misalnya, `172.16.1.1/32`). Tujuan tidak boleh berupa rentang IP VPC tempat tabel rute berada karena rute lokal telah mengizinkan interkoneksi jaringan pribadi di VPC ini.
Jenis hop selanjutnya	Menunjukkan jalan keluar dari paket data untuk VPC. Jenis yang didukung: NAT Gateway: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke NAT Gateway. Peering Connections: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke pasangan VPC untuk peering connection. Direct Connect Gateway: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke direct connect gateway. IP Virtual Ketersediaan Tinggi: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke HAVIP. VPN Gateway: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke VPN gateway. IP publik CVM: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke IP publik (termasuk EIP) untuk instans CVM di VPC. CVM: lalu lintas yang diarahkan ke rentang IP tujuan diteruskan ke instans CVM di VPC.
Hop selanjutnya	Menentukan instans hop selanjutnya yang menjadi tujuan pengalihan lalu lintas, seperti gateway atau IP CVM.
Catatan	(Opsional) Anda dapat memasukkan deskripsi rute untuk pengelolaan sumber daya.
Tambahkan jalur	Anda dapat mengklik +**Tambahkan jalur** untuk mengonfigurasi beberapa kebijakan perutean, atau mengklik ikon penghapusan di kolom **Operasi** untuk menghapus kebijakan perutean yang tidak perlu.



5. Klik **Create(Buat)**.

Mengedit Kebijakan Perutean

1. Login ke konsol VPC, dan akses halaman **Route Table** (Tabel Rute).
2. Dalam daftar, klik **ID/Name** (ID/Nama) dari tabel rute target untuk membuka halaman detailnya.
3. Klik **Edit** (Edit) di kolom **Operation** (Operasi) dari kebijakan perutean untuk memodifikasinya.



4. Setelah modifikasi, klik **OK** (OKE) untuk menyimpan atau **Cancel** (Batalkan) untuk menghapus hasil modifikasi.

Memublikasikan/Menarik Kebijakan Perutean ke/dari CCN

Rute VPC yang dikaitkan dengan CCN dipublikasikan ke CCN secara default. Untuk kebijakan perutean kustom baru yang tidak dipublikasikan, Anda perlu memublikasikannya secara manual. Anda juga dapat menarik kebijakan perutean dari CCN.

Saat ini, hanya kebijakan perutean dengan **Next hop type** (Jenis hop selanjutnya) yang memiliki **High Availability Virtual IP** (IP Virtual Ketersediaan Tinggi) atau **CVM** (CVM) dalam tabel rute default atau kustom yang dapat dipublikasikan secara manual ke atau ditarik dari CCN.

Prasyarat

VPC tempat HAVIP atau CVM berada dikaitkan dengan instans CCN.

Petunjuk

1. Login ke konsol VPC, dan akses halaman **Route Table** (Tabel Rute).
2. Klik **ID/Name** (ID/Nama) dari tabel rute yang akan dimodifikasi untuk membuka halaman detailnya.
3. Lakukan operasi berikut sesuai kebutuhan:

Klik **Publish to CCN** (Publikasikan ke CCN) untuk memublikasikan kebijakan perutean kustom secara manual ke CCN.

Klik **Withdraw from CCN** (Tarik dari CCN) untuk menarik kebijakan perutean kustom yang telah dipublikasikan ke CCN.

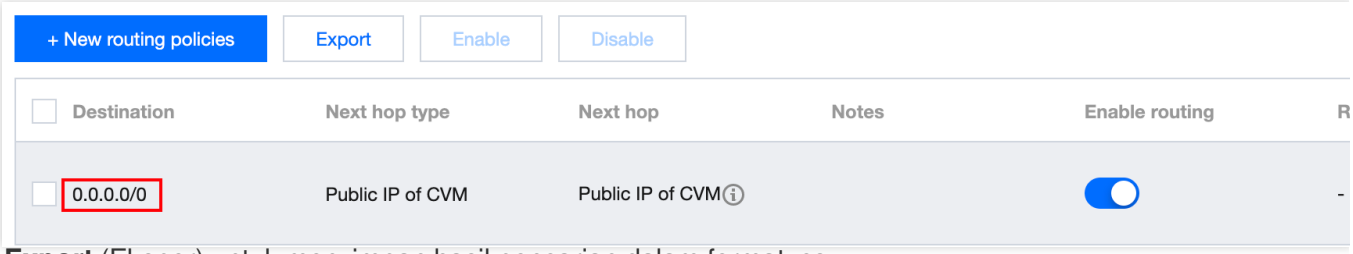
Perhatian:

Kebijakan perutean yang dinonaktifkan tidak dapat dipublikasikan ke CCN.

Kebijakan perutean tidak dapat dinonaktifkan setelah dipublikasikan ke CCN.

Mengkueri dan Mengekspor Kebijakan Perutean

1. Login ke konsol VPC, dan akses halaman **Route Table** (Tabel Rute).
2. Klik **ID/Name** (ID/Nama) dari tabel rute target untuk membuka halaman detailnya. Di halaman ini, Anda dapat melihat kebijakan perutean di tabel rute ini.
3. Pada kotak pencarian di kanan atas, Anda dapat mengkueri kebijakan perutean dengan memasukkan alamat tujuan.



4. Klik **Export** (Ekspor) untuk menyimpan hasil pencarian dalam format .csv.

Mengaktifkan/Menonaktifkan Kebijakan Perutean

Kebijakan perutean kustom dapat diaktifkan atau dinonaktifkan.

Petunjuk

1. Login ke konsol VPC, dan akses halaman **Route Table** (Tabel Rute).
2. Klik **ID/Name** (ID/Nama) dari tabel rute target untuk masuk ke halaman detailnya. Periksa status kebijakan perutean:


: diaktifkan

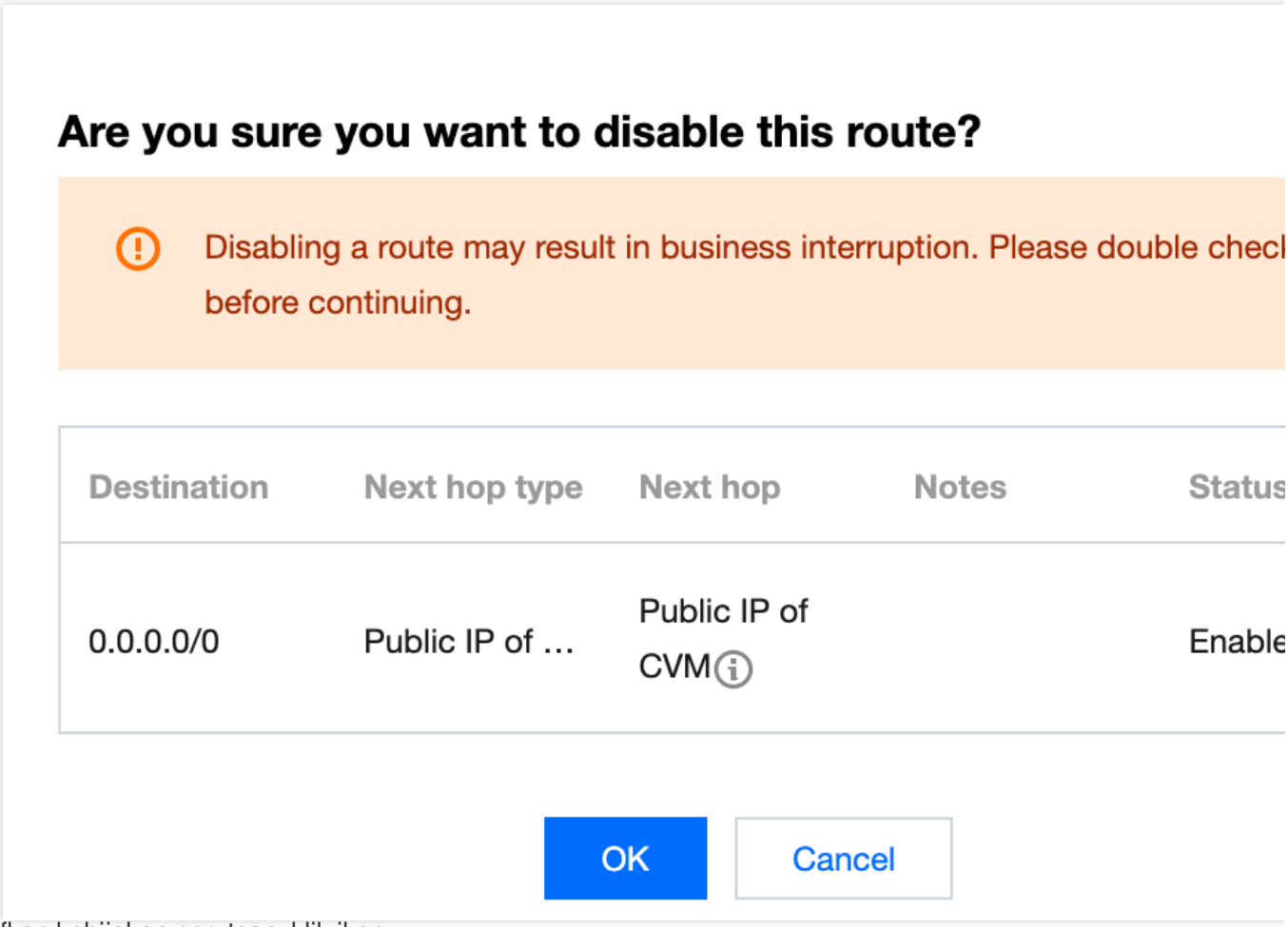

: dinonaktifkan

3. Nonaktifkan kebijakan perutean: klik ikon


di samping kebijakan perutean untuk menonaktifkannya.

Perhatian:

Menonaktifkan rute dapat mengakibatkan gangguan bisnis. Harap periksa kembali sebelum melanjutkan.

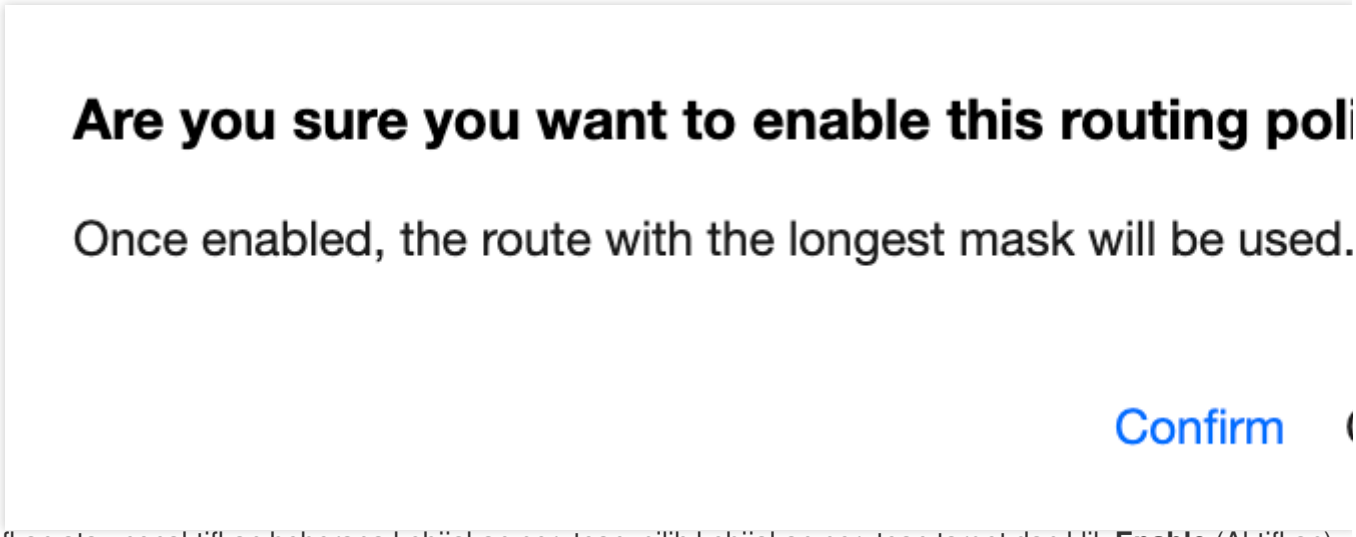


4. Aktifkan kebijakan perutean: klik ikon

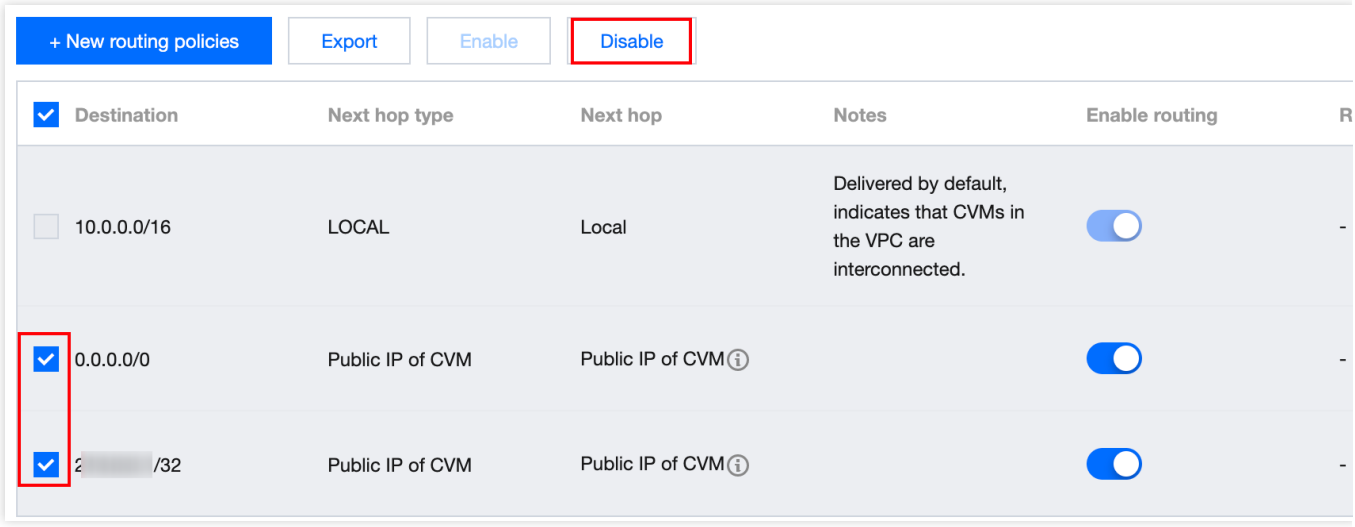
di samping kebijakan perutean untuk mengaktifkannya.

Perhatian:

Setelah diaktifkan, rute dengan mask terpanjang akan digunakan. Hal ini dapat memengaruhi bisnis Anda saat ini. Harap periksa kembali sebelum melanjutkan.



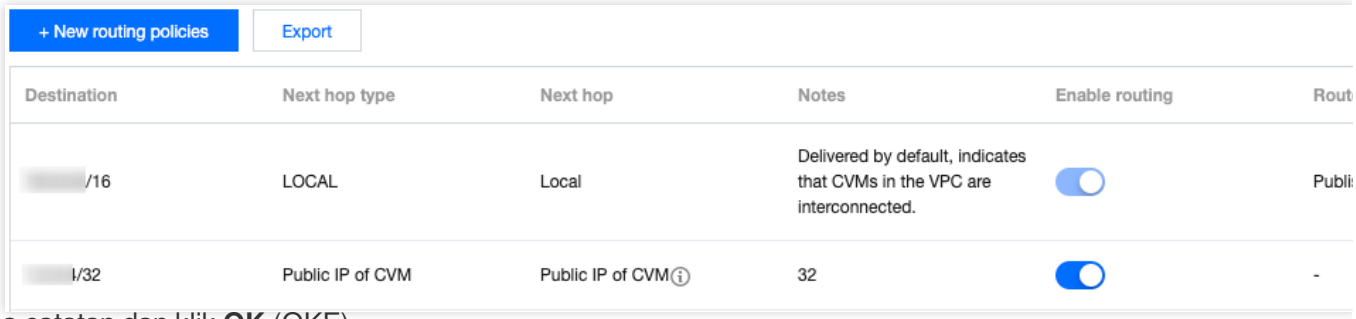
5. Aktifkan atau nonaktifkan beberapa kebijakan perutean: pilih kebijakan perutean target dan klik **Enable** (Aktifkan) atau **Disable** (Nonaktifkan) di atas daftar.



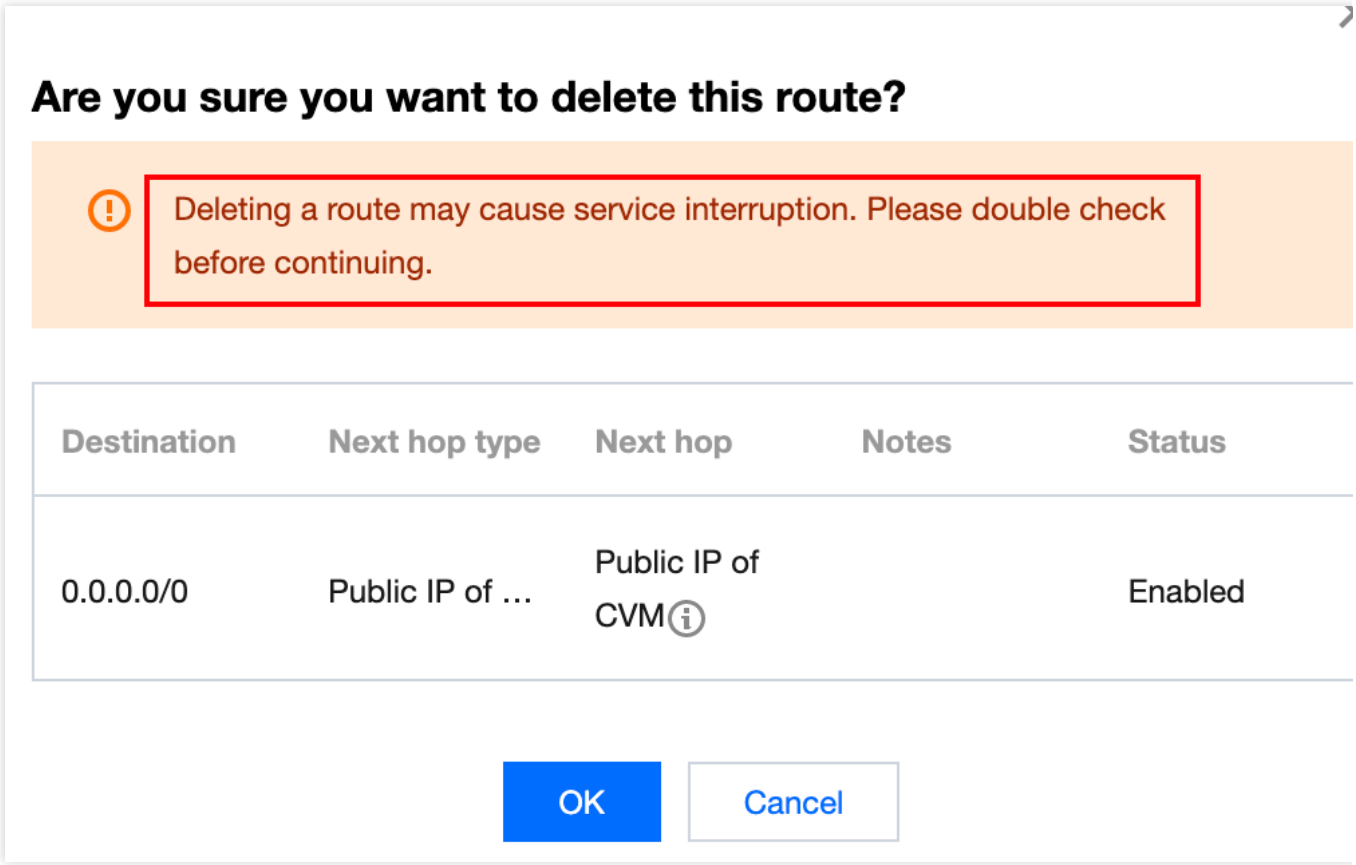
Menghapus Kebijakan Perutean

Anda dapat menghapus kebijakan perutean yang tidak digunakan. Hanya kebijakan perutean kustom yang dapat dihapus.

1. Login ke konsol VPC, dan akses halaman **Route Table** (Tabel Rute).
2. Klik **ID/Name** (ID/Nama) dari tabel rute yang akan dimodifikasi untuk membuka halaman detailnya.
3. Pilih kebijakan perutean yang akan dihapus, dan klik **Delete** (Hapus) di bawah kolom **Operation** (Operasi).



4. Baca catatan dan klik **OK** (OKE).



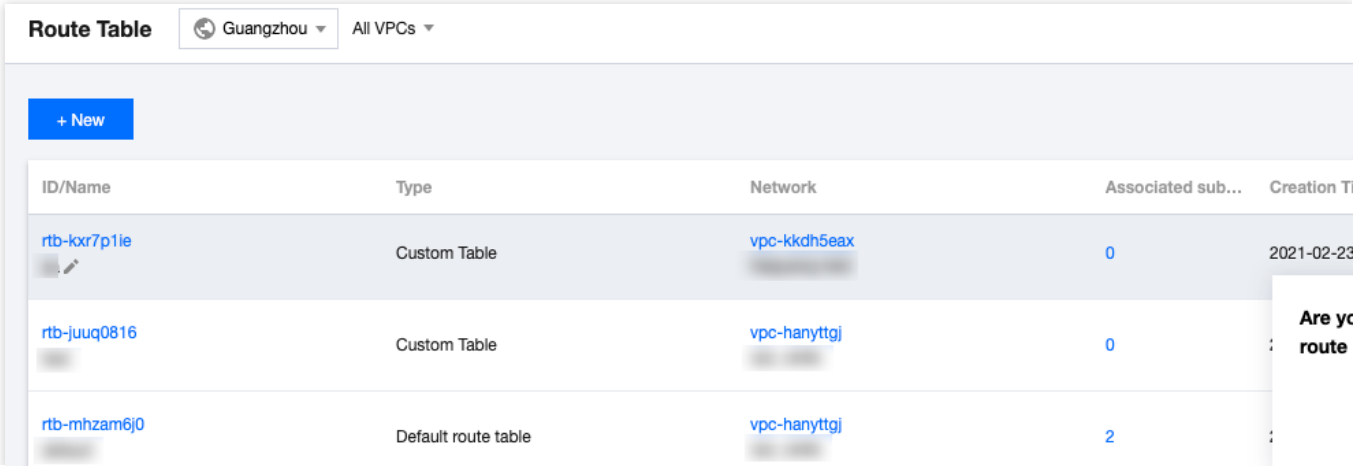
Menghapus Tabel Perutean

Waktu update terbaru：2024-01-24 17:48:51

Anda dapat menghapus tabel rute yang tidak terhubung dengan subnet apa pun. Anda hanya dapat menghapus tabel rute kustom, bukan tabel rute default yang dibuat secara otomatis oleh sistem.

Petunjuk

1. Login ke konsol VPC, dan pilih **Route Table** (Tabel Rute).
2. Dalam daftar, pilih tabel rute yang akan dihapus. Klik **Delete** (Hapus) di kolom **Operation** (Operasi).



IP dan ENI

IP Elastis

Waktu update terbaru：2024-01-24 17:48:51

Elastic IP (EIP): EIP adalah alamat IP statis yang dirancang khusus untuk komputasi cloud. Ini juga merupakan alamat IP publik yang tetap tidak berubah di suatu wilayah. Dengan EIP, Anda dapat memetakan kembali alamat ke instans lain dengan cepat atau instans gateway NAT di akun Anda agar instans tidak mengalami kegagalan.
Anda dapat menyimpan EIP di akun Anda hingga dirilis. Sementara IP publik hanya dapat dirilis dengan CVM, EIP dapat dipisahkan dari siklus pemakaian CVM dan beroperasi secara independen sebagai sumber daya cloud. Misalnya, jika Anda perlu mempertahankan IP publik yang sangat terkait dengan bisnis, Anda dapat mengubahnya menjadi EIP dan menyimpannya di akun Anda.
Untuk pengoperasian EIP langkah demi langkah, lihat bagian “Petunjuk” di Elastic IP.

HAVIP

Ikhtisar

Waktu update terbaru：2024-01-24 17:48:51

IP virtual ketersediaan tinggi (HAVIP) adalah alamat IP pribadi yang ditetapkan dari blok CIDR dari subnet VPC. Alamat ini biasanya digunakan bersama perangkat lunak dengan ketersediaan tinggi, seperti Keepalived dan Windows Server Failover Cluster, untuk membangun kluster utama/sekunder dengan ketersediaan tinggi.

Keterangan:

HAVIP saat ini dalam versi beta, dan peralihan antara server utama/sekunder mungkin memerlukan waktu 10 detik. Untuk mencobanya, harap ajukan permohonan untuk menjadi pengguna beta.

Untuk menjamin ketersediaan tinggi CVM di kluster utama/sekunder, Anda sebaiknya menetapkan CVM ke host yang berbeda menggunakan grup penempatan. Untuk informasi selengkapnya tentang grup penempatan, lihat Grup Penempatan.

Perangkat lunak ketersediaan tinggi harus mendukung pengiriman pesan ARP.

Fitur

Anda dapat mengajukan beberapa alamat HAVIP di konsol untuk setiap VPC.

Anda harus mengikat HAVIP di file konfigurasi CVM.

Arsitektur dan Prinsip

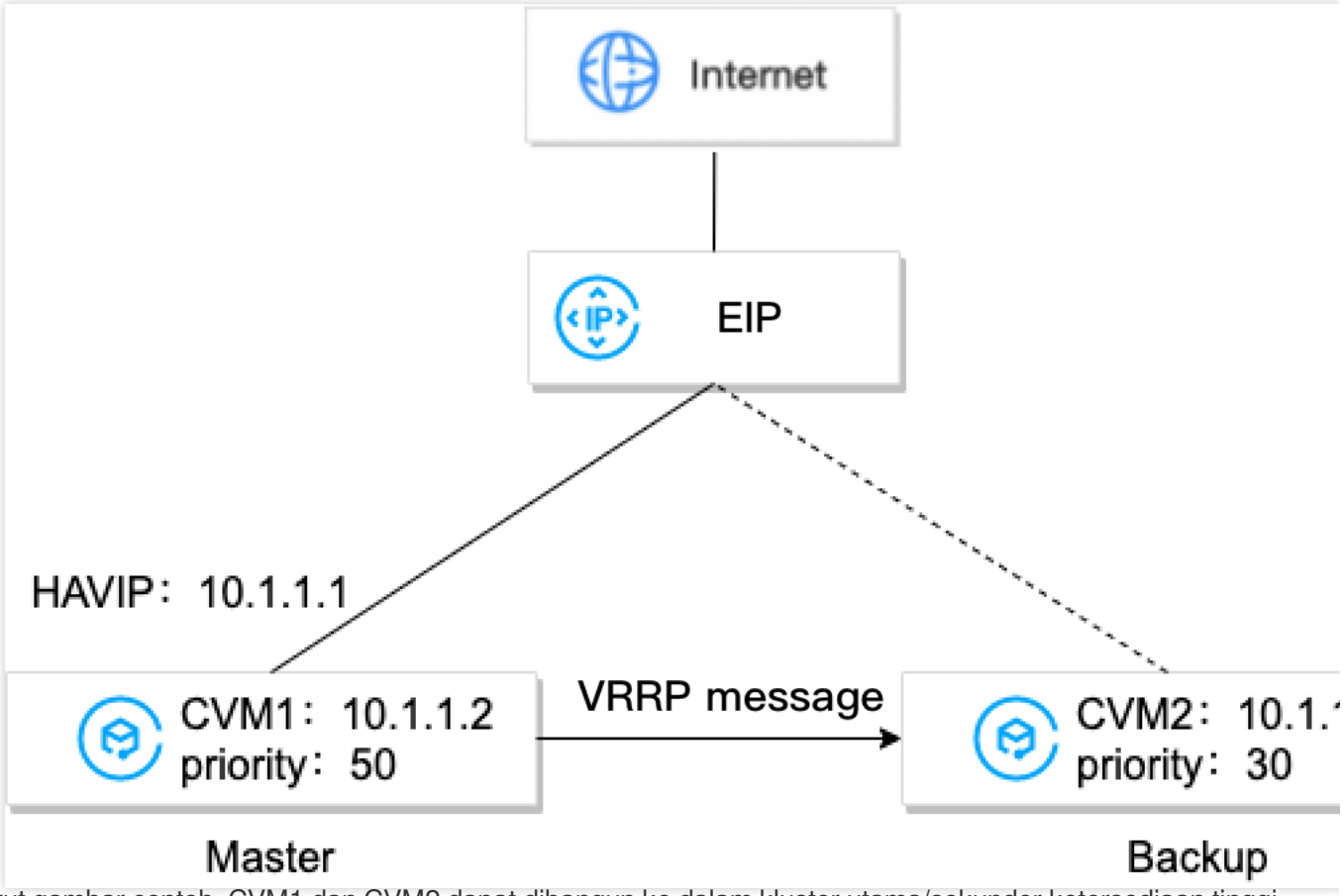
Biasanya, kluster utama/sekunder ketersediaan tinggi terdiri dari dua server: server utama aktif dan server sekunder siaga. Kedua server memiliki VIP (IP virtual) yang sama. VIP hanya dapat bekerja di satu server utama pada saat bersamaan. Ketika server utama gagal, server sekunder akan mengambil alih VIP untuk terus menyediakan layanan. Dalam jaringan fisik tradisional, status utama/sekunder dapat dinegosiasikan dengan protokol VRRP Keepalived. Perangkat utama mengirimkan pesan ARP gratis secara berkala untuk membersihkan tabel MAC atau tabel ARP terminal dari pertukaran uplink, sehingga memicu migrasi VIP ke perangkat utama.

Dalam VPC, kluster utama/sekunder ketersediaan tinggi juga dapat diimplementasikan dengan men-deploy Keepalived di CVM. Namun, instans CVM biasanya tidak dapat memperoleh IP pribadi melalui pengumuman ARP karena alasan keamanan seperti spoofing ARP. VIP harus HAVIP yang diterapkan dari Tencent Cloud yang berbasis subnet. Dengan demikian, HAVIP hanya dapat diikat ke server di subnet yang sama melalui pengumuman.

Keterangan:

Keepalived adalah perangkat lunak ketersediaan tinggi berbasis VRRP. Untuk menggunakan Keepalived, pertama selesaikan konfigurasinya di file `Keepalived.conf` .

Gambar berikut menunjukkan arsitektur HAVIP.



Menurut gambar contoh, CVM1 dan CVM2 dapat dibangun ke dalam kluster utama/sekunder ketersediaan tinggi dengan langkah-langkah berikut:

1. Instal Keepalived di CVM1 dan CVM2, konfigurasikan HAVIP sebagai VRRP VIP, dan tetapkan prioritas server utama dan sekunder. Nilai yang lebih besar merepresentasikan prioritas yang lebih tinggi.
2. Keepalived menggunakan protokol VRRP untuk membandingkan prioritas awal CVM1 dan CVM2 dan menentukan CVM1 sebagai server utama karena prioritasnya yang lebih tinggi.
3. Server utama mengirimkan pesan ARP, mengumumkan VIP (HAVIP), dan memperbarui pemetaan VIP ke mac. Dalam hal ini, CVM1 adalah server utama dan menyediakan layanan dengan menggunakan IP pribadi (HAVIP) untuk komunikasi. Anda dapat melihat HAVIP terikat ke server utama CVM1 di konsol HAVIP.
4. (Opsional) Ikat EIP ke HAVIP di konsol untuk menerapkan komunikasi melalui jaringan publik.
5. Server utama mengirimkan pesan VRRP ke server sekunder secara berkala. Jika server utama gagal mengirim pesan VRRP dalam jangka waktu tertentu, server sekunder akan ditetapkan sebagai utama dan mengirimkan pesan pembaruan ARP yang membawa alamat MAC-nya. Dalam hal ini, CVM2 menjadi server utama untuk menyediakan layanan komunikasi dan menangani permintaan akses eksternal. Anda akan melihat bahwa CVM yang diikatkan ke HAVIP berubah menjadi CVM2 pada konsol HAVIP.

Kasus Penggunaan Umum

Cloud load balancer HA

Untuk men-deploy Cloud Load Balancers (CLB), Anda biasanya akan menggunakan HA antar instans CLB dan mengonfigurasi server nyata sebagai kluster. Dengan demikian, Anda harus men-deploy dan menggunakan HAVIP sebagai IP virtual antara dua server CLB.

Database relasional utama/sekunder

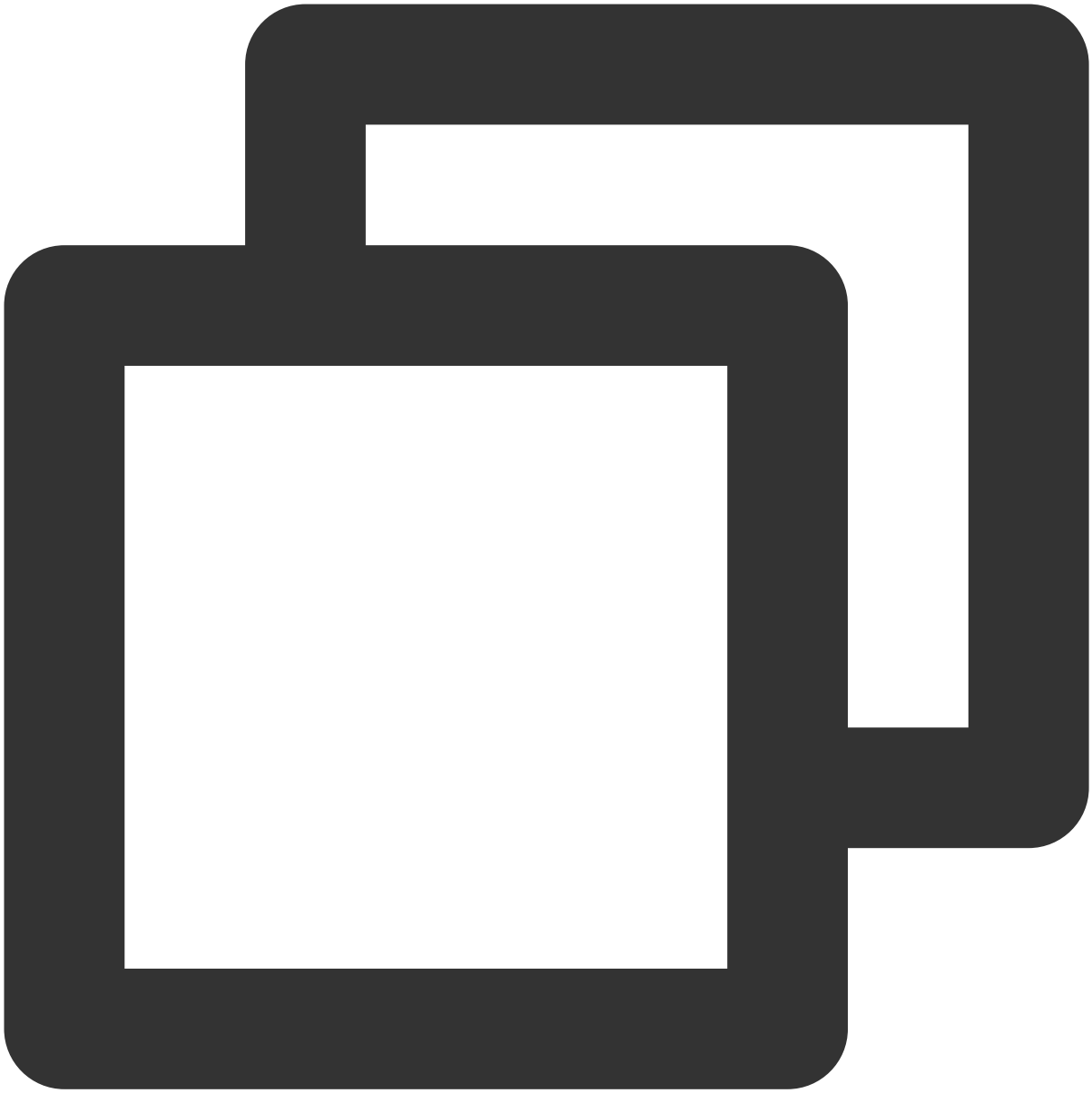
Jika Keepalived atau Windows Server Failover Cluster digunakan di antara dua database untuk membangun kluster utama/sekunder dengan ketersediaan tinggi, gunakan HAVIP sebagai IP virtual. Untuk informasi selengkapnya, lihat Membangun Kluster Utama/Sekunder Ketersediaan Tinggi Menggunakan HAVIP + Keepalived dan Membuat Database Ketersediaan Tinggi dengan Menggunakan HAVIP + Kluster Failover Server Windows pada Praktik Terbaik.

Pertanyaan Umum

Mengapa saya harus menggunakan HAVIP bersama Keepalive di VPC?

Beberapa vendor cloud publik tidak mendukung pengikatan IP pribadi ke CVM melalui pengumuman ARP karena alasan keamanan seperti spoofing ARP. Jika Anda langsung menggunakan IP pribadi sebagai IP virtual di file “Keepalived.conf”, Keepalived tidak akan dapat memperbarui pemetaan IP ke MAC selama peralihan IP virtual server utama/sekunder. Dalam hal ini, Anda harus memanggil API untuk mengganti IP.

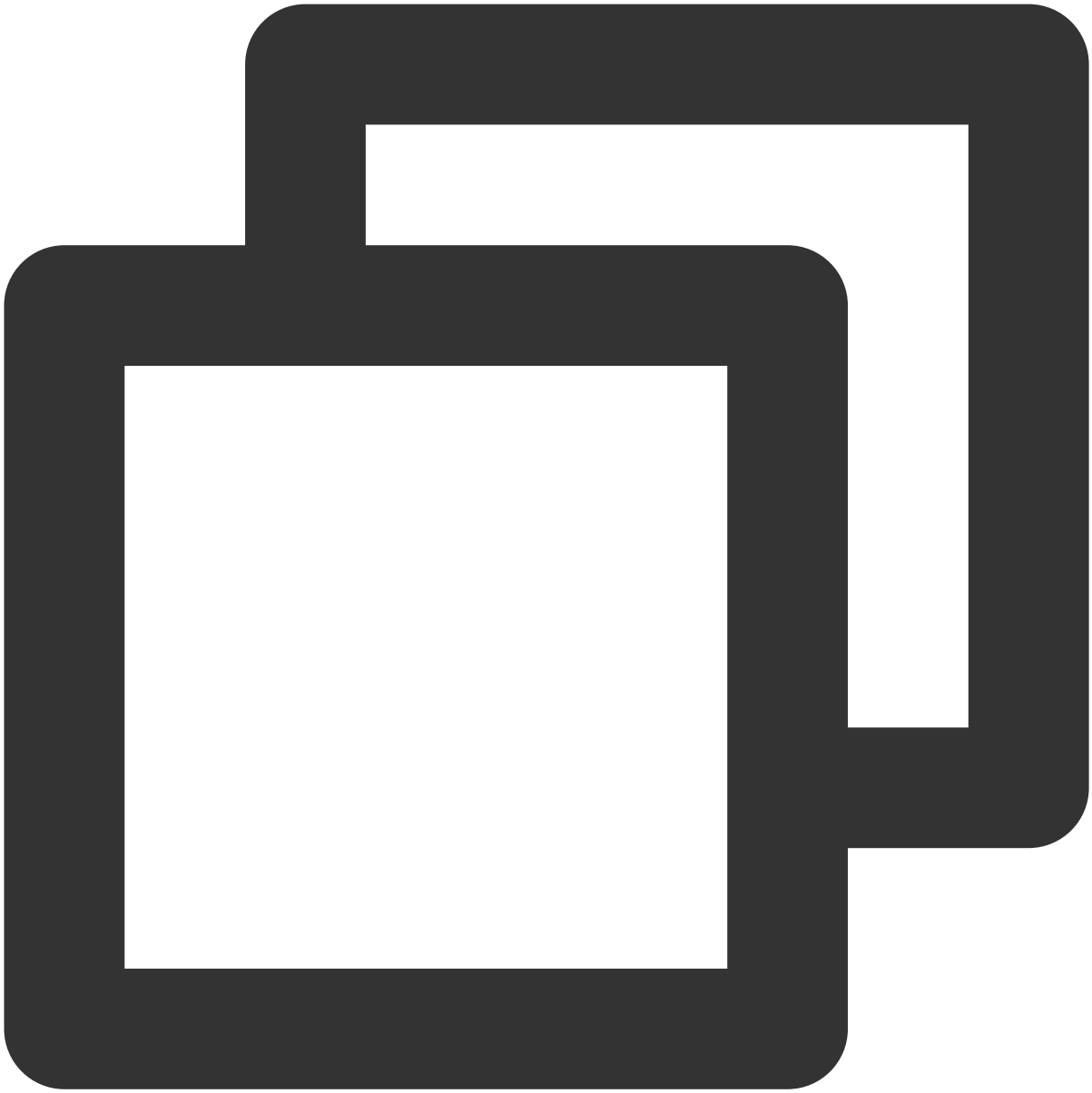
Menggunakan konfigurasi Keepalived sebagai contoh, konfigurasi IP adalah sebagai berikut:



```
vrrp_instance VI_1 {
    state BACKUP            #Perangkat sekunder
    interface eth0           #nama ENI
    virtual_router_id 51
    nopreempt                    #Mode Non-preempt
    #preempt_delay 10
    priority 80
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
```

```
    }
    unicast_src_ip 172.17.16.7 #IP pribadi perangkat lokal
    unicast_peer {
        172.17.16.13           #Alamat IP dari perangkat pasangan, misalnya: 10.0.0
    }

    virtual_ipaddress {

        172.17.16.3 #Masukkan alamat HAVIP yang telah diterapkan di konsol.

    }

    garp_master_delay 1
    garp_master_refresh 5

    track_interface {
        eth0
    }

    track_script {
        checkhaproxy
    }
}
```

Jika tidak ada HAVIP, bagian berikut dari file konfigurasi akan tidak valid.



```
virtual_ipaddress {
   172.17.16.3 #Masukkan alamat HAVIP yang telah diterapkan di konsol.
}
```

Referensi

Untuk informasi selengkapnya tentang batas HAVIP, lihat Batas.

Untuk informasi selengkapnya tentang panduan pengoperasian HAVIP, lihat Mengelola HAVIP.

Batasan

Waktu update terbaru：2024-01-24 17:48:52

Batasan Penggunaan

Penempatan HAVIP dapat ditentukan oleh CVM backend, tetapi Anda tidak dapat secara manual mengikat HAVIP ke server tertentu di konsol (pengalaman sejalan dengan komputer fisik tradisional.)
RS backend tetapi bukan HAVIP yang menentukan apakah akan bermigrasi berdasarkan negosiasi file konfigurasi.
Hanya instans VPC yang didukung, dan jaringan dasar tidak didukung.
Deteksi heartbeat harus dilakukan oleh aplikasi pada CVM, tetapi tidak oleh HAVIP yang hanya berfungsi sebagai alamat IP floating yang ditentukan oleh ARP (pengalaman sejalan dengan mesin fisik tradisional.)

Batasan Kuota

Sumber daya	Batas
Kuota HAVIP default di setiap VPC	10

Mengelola HAVIP

Waktu update terbaru：2024-01-24 17:48:51

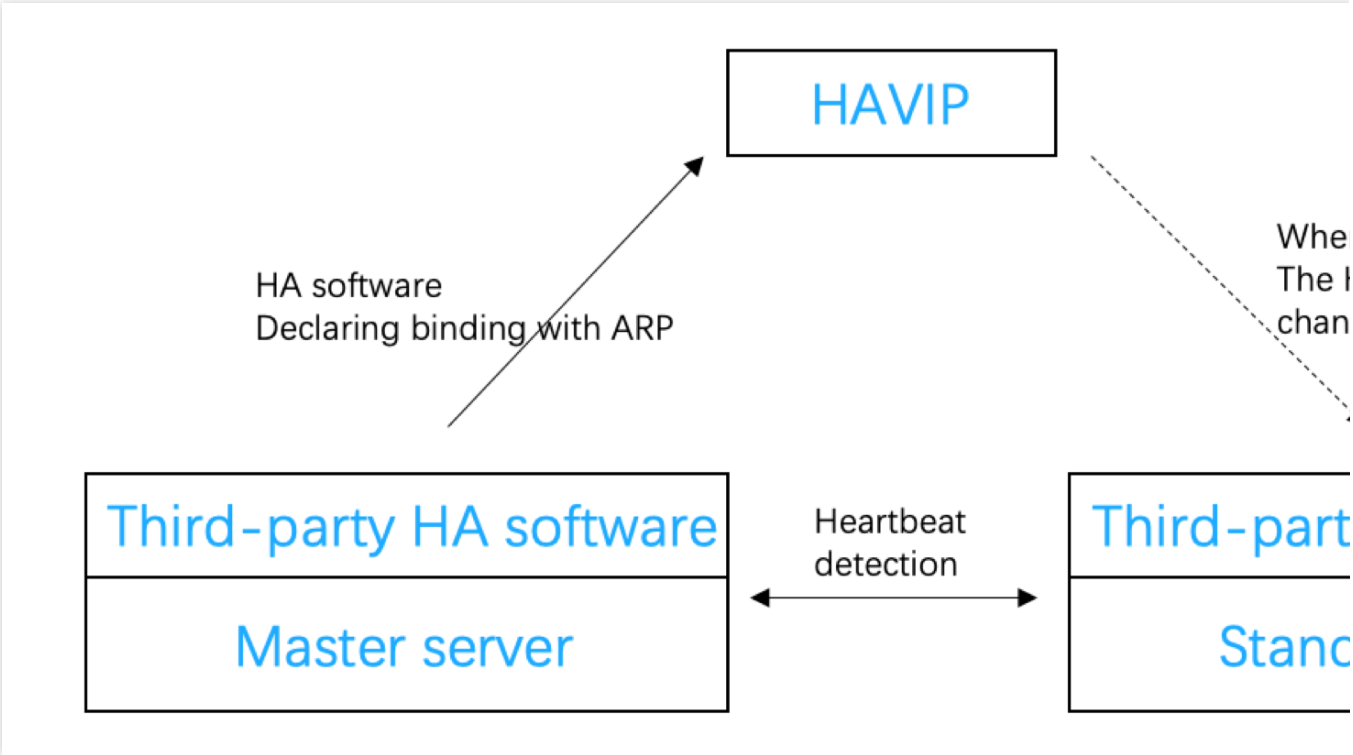
Dokumen ini menjelaskan cara membuat HAVIP di konsol dan mengonfigurasinya di perangkat lunak pihak ketiga.

Petunjuk

1. Login ke konsol VPC dan pilih **IP and Interface** (IP dan Antarmuka) > **HAVIP** di bilah sisi kiri.
2. Pilih wilayah target di halaman pengelolaan HAVIP dan klik **Apply** (Terapkan).
3. Pada kotak dialog pop-up, konfigurasikan parameter HAVIP.
Name (Nama): masukkan nama untuk HAVIP.
Virtual Private Cloud: pilih VPC tempat HAVIP yang akan dibuat.
Subnet: pilih subnet untuk HAVIP yang spesifik untuk subnet.
IP address (Alamat IP): alamat IP HAVIP dapat ditetapkan secara otomatis atau ditentukan secara manual. Jika Anda memilih **Automatic Assignment** (Penetapan Otomatis), alamat IP subnet akan ditetapkan secara otomatis. Jika Anda memilih **Enter manually** (Masukkan secara manual), pastikan alamat IP yang dimasukkan berada dalam rentang IP subnet dan bukan alamat IP yang dicadangkan dari sistem. Misalnya, jika rentang IP subnet adalah `10.0.0.0/24`, alamat IP pribadi yang dimasukkan harus berada dalam `10.0.0.2-10.0.0.254`.
4. Klik **OK** (OKE). Setelah berhasil dibuat, HAVIP akan ditampilkan dalam daftar, dan statusnya adalah **Not bound with CVM yet** (Belum diikatkan dengan CVM).

Mengonfigurasi HAVIP

HAVIP dirancang untuk digunakan bersama dengan perangkat lunak HA pihak ketiga yang harus dikonfigurasi dalam perangkat lunak HA pihak ketiga. HAVIP hanya merupakan objek operasi dan alamat IP pribadi yang dapat diikatkan melalui pengumuman. Dengan demikian, pengikatan dan pemutusan ikatan HAVIP ke CVM tidak dilakukan di konsol Tencent Cloud. Sebagai gantinya, Anda hanya perlu menentukan HAVIP sebagai alamat IP virtual floating (VIP) di perangkat lunak HA pihak ketiga yang kemudian menentukan ENI untuk dikaitkan ke HAVIP melalui ARP. Berikut ini adalah cara mengikat atau memutuskan ikatan HAVIP:

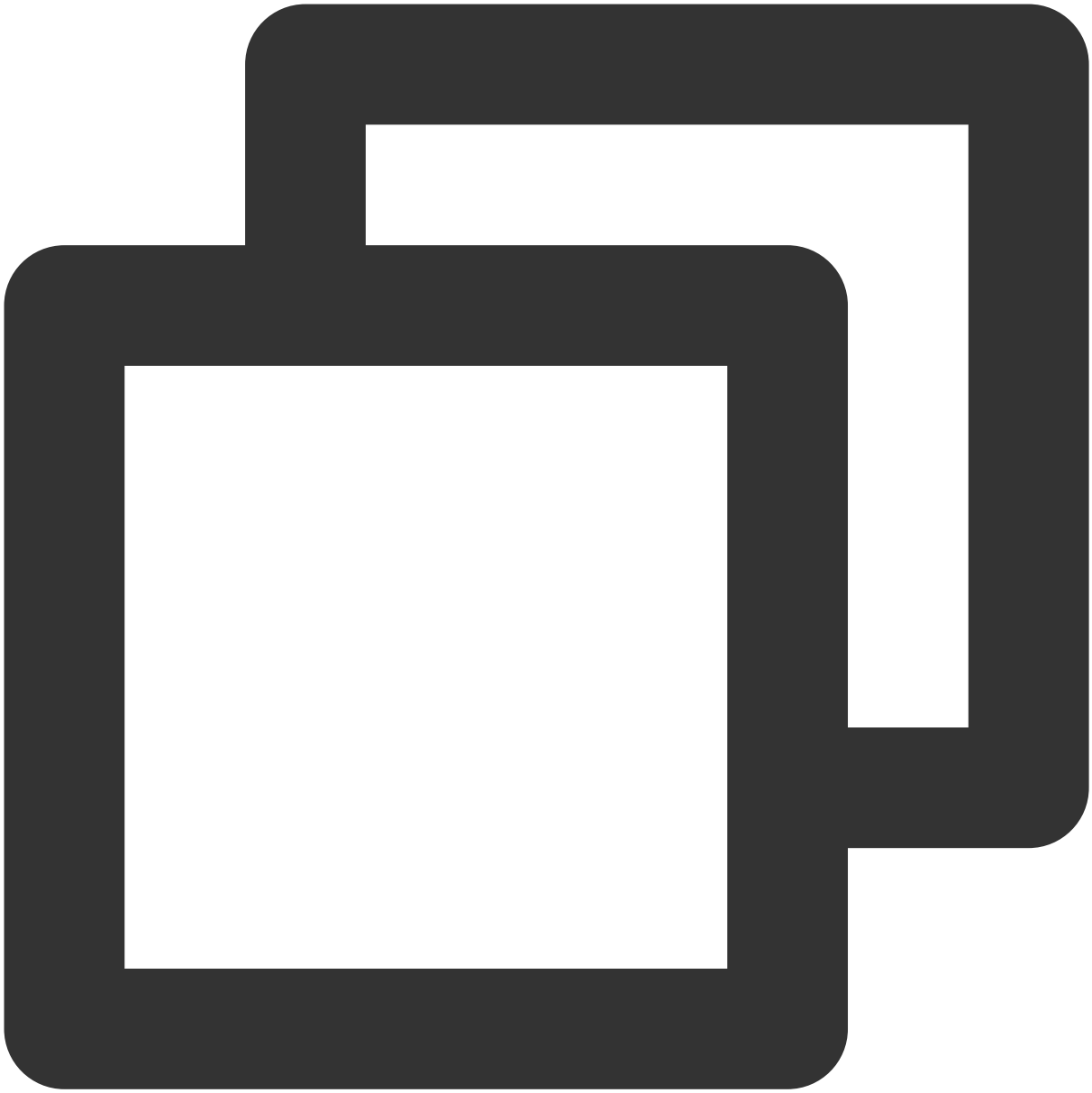


Dalam lingkungan perangkat fisik tradisional, semua alamat IP pribadi diikat ke ENI melalui ARP secara default dan dapat ditentukan sebagai alamat IP floating dalam perangkat lunak HA. Di lingkungan cloud publik, IP pribadi tidak dapat menggunakan ARP, atau ditetapkan sebagai alamat IP floating di perangkat lunak HA. Dengan demikian, Anda harus mengikuti langkah yang sama dengan perangkat lunak pihak ketiga untuk menentukan HAVIP sebagai alamat IP floating.

Keterangan:

Program perangkat lunak HA umum meliputi: Linux HeartBeat, Keepalived, Pacemaker, dan Windows MSCS.

Saat menentukan VIP di file konfigurasi perangkat lunak HA, Anda hanya perlu memasukkan HAVIP yang Anda buat:



```
vrrp_instanceVI_1 {
# Pilih parameter yang tepat untuk CVM utama dan sekunder.
    state MASTER               #Atur status awal ke `Pencadangan`.
    interface eth0              #ENI seperti `eth0` digunakan untuk mengikat VIP
    virtual_router_id 51        #Nilai untuk kluster `virtual_router_id`
        nopreempt                   #Mode Non-preempt
        preempt_delay 10           #Atur penundaan ke 10 menit
    priority 100               #Prioritas. Semakin besar nilai, semakin tinggi prio
    advert_int 1               #Periksa interval. Nilai default adalah 1 detik
    authentication {           #Autentikasi
        auth_type PASS          #Metode autentikasi
```

```
        auth_pass 1111          #Kata sandi autentikasi
    }
        unicast_src_ip 172.16.16.5 #Alamat IP pribadi perangkat lokal
        unicast_peer{
        172.16.16.6                #alamat IP perangkat pasangan
        }
    virtual_ipaddress {
        172.16.16.12               #HAVIP
    }
    }
```

Setelah konfigurasi selesai di perangkat lunak HA CVM, status HAVIP akan berubah menjadi **Bound with CVM** (Terikat ke CVM) di konsol.

Lihat kasus berikut untuk konfigurasi Anda:

Keterangan:

Membangun Kluster Utama/Sekunder HA Menggunakan HAVIP + Keepalived

Membuat Database HA Menggunakan HAVIP + Windows Server Failover Cluster

Dokumentasi

Mirip dengan IP pribadi, HAVIP juga dapat diikat dengan atau diputuskan ikatannya dari EIP di konsol. Jika Anda memerlukan komunikasi jaringan publik, lihat Mengikat atau Memutuskan Ikatan EIP.

Mengikat atau Memutuskan Ikatan EIP

Waktu update terbaru：2024-01-24 17:48:51

Mirip dengan IP pribadi, pengikatan HAVIP juga dapat dikonfigurasi di konsol. Pengikatan HAVIP mengacu pada operasi EIP. Anda dapat melewati bagian ini jika tidak diperlukan koneksi jaringan publik.

Pengikatan EIP

1. Login ke konsol VPC dan pilih **IP and Interface** (IP dan Antarmuka) > **HAVIP** di bilah sisi kiri.
2. Pilih wilayah target pada halaman pengelolaan HAVIP.
3. Pilih HAVIP yang akan diikat ke EIP, dan klik **Bind** (Ikatkan) di kolom **Operation** (Operasi).
4. Pada kotak dialog pop-up, pilih EIP yang akan diikatkan.

Perhatian:

Satu HAVIP hanya dapat diikatkan ke satu EIP. Jika tidak ada EIP yang tersedia, Anda harus terlebih dahulu membuat EIP di konsol.

Jika HAVIP tidak dibatasi dengan instans CVM, EIP terkait akan berstatus tidak aktif dan akan dikenakan biaya waktu jeda. Harap konfigurasi HAVIP dengan benar dan ikat ke instans dengan mengacu pada kasus berikut:

Membangun Kluster Utama/Sekunder Ketersediaan Tinggi dengan Menggunakan HAVIP + Keepalived di Praktik Terbaik

Membuat Database Ketersediaan Tinggi dengan Menggunakan HAVIP + Windows Server Failover Cluster di Praktik Terbaik

5. Klik **OK** (OKE).

Memutuskan Ikatan EIP

1. Login ke konsol VPC dan pilih **IP and Interface** (IP dan Antarmuka) > **HAVIP** di bilah sisi kiri.
2. Pilih wilayah target pada halaman pengelolaan HAVIP.
3. Pilih HAVIP dari tempat ikatan EIP akan dilepas, dan klik **Unbind** (Memutuskan Ikatan) di kolom **Operation** (Operasi).
4. Pada jendela pop-up, baca catatan, dan klik **OK** (OKE) untuk memutuskan ikatan EIP.

Perhatian:

Bisnis jaringan publik Anda mungkin terpengaruh setelah memutuskan ikatan EIP. Harap bersiap sejak awal.

Setelah ikatan diputuskan, EIP akan menjeda dan membebankan biaya waktu jeda. Anda dapat langsung merilis EIP yang tidak digunakan untuk menghindari biaya.

Mengkueri HAVIP

Waktu update terbaru：2024-01-24 17:48:51

Anda dapat melihat semua detail HAVIP di wilayah tertentu di konsol HAVIP.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih **IP and Interface** (IP dan Antarmuka) > **HAVIP** di bilah sisi kiri untuk masuk ke halaman pengelolaan HAVIP.
3. Pilih wilayah target untuk melihat detail semua HAVIP yang telah diajukan.
 Deskripsi bidang adalah sebagai berikut:
ID/Nama: ID mengacu pada ID HAVIP yang dibuat secara otomatis setelah dibuat. Anda dapat mengekliknya untuk melihat informasi dasar HAVIP. Nama ditentukan oleh pengguna saat HAVIP dibuat.
Status: menunjukkan apakah HAVIP ditetapkan sebagai alamat IP floating di file konfigurasi perangkat lunak HA di CVM. HAVIP yang berhasil dikonfigurasi akan berstatus **Bound with CVM** (Terikat dengan CVM), atau berstatus **Not bound with CVM yet** (Belum terikat dengan CVM).
Alamat: alamat HAVIP.
Backend ENI: mengacu pada ID ENI dari CVM terikat. Jika HAVIP belum terikat dengan CVM, bidang ini akan ditampilkan sebagai **-**.
Server: mengacu pada ID CVM terikat. Jika HAVIP belum terikat dengan CVM, bidang ini akan ditampilkan sebagai **-**.
EIP: mengacu pada EIP terikat. Jika HAVIP belum terikat dengan EIP, bidang ini akan ditampilkan sebagai **-**.
Virtual Private Cloud: mengacu pada VPC dari HAVIP.
Subnet: mengacu pada subnet HAVIP.
Waktu Aplikasi: mengacu pada waktu saat HAVIP ini diterapkan.
Operasi: mengacu pada operasi yang didukung, termasuk **Bind** (Ikatkan), **Unbind** (Putuskan Ikatan), dan **Release** (Rilis).
Ikatkan: mengikat EIP
Putuskan ikatan: memutuskan ikatan EIP
Rilis: merilis HAVIP
4. Masukkan ID, nama atau alamat di kotak pencarian di sebelah kanan untuk mencari HAVIP dengan cepat.
5. Klik ikon di sebelah kotak pencarian untuk memuat ulang halaman.

Melepaskan HAVIP

Waktu update terbaru：2024-01-24 17:48:51

Dokumen ini menjelaskan cara merilis HAVIP yang tidak digunakan.

Prasyarat

Hanya HAVIP yang **not bound with CVM** (tidak terikat dengan CVM) yang dapat dirilis.
Keterangan:
Untuk HAVIP yang **bound with CVM** (terikat dengan CVM), Anda perlu melepas ikatan HAVIP di file konfigurasi perangkat lunak HA pihak ketiga di CVM sebelum merilisnya di konsol.

Petunjuk

1. Login ke Konsol VPC.
2. Pilih **IP and Interface** (IP dan Antarmuka) > **HAVIP** di bilah sisi kiri. Dalam daftar HAVIP, temukan HAVIP yang akan dirilis.
3. Klik **Release** (Rilis) di kolom **Operation** (Operasi).
4. Klik **Confirm** (Konfirmasi) di kotak dialog pop-up.

ENI

Waktu update terbaru：2024-01-24 17:48:51

Elastic Network Interface (ENI) terikat ke CVM dalam VPC dan dapat dimigrasikan antara CVM secara bebas. ENI membantu Anda mengonfigurasi jaringan pengelolaan dan membuat solusi jaringan yang sangat andal.
Anda dapat mengikat beberapa ENI di zona ketersediaan yang sama ke CVM berdasarkan spesifikasi CVM untuk memastikan jaringan yang sangat tersedia. Anda juga dapat mengikat beberapa alamat IP pribadi ke ENI untuk men-deploy beberapa alamat IP untuk satu CVM.
Untuk operasi umum ENI, harap lihat:
Membuat ENI
Mengikat dan Mengonfigurasi CVM
Memutuskan ikatan dari CVM
Menghapus ENI
Mengikat Alamat IP Pribadi Sekunder
Merilis Alamat IP Pribadi Sekunder
Mengikat EIP
Memutuskan Ikatan EIP
Menyesuaikan Alamat IP Pribadi Utama
Mengubah Subnet ENI

Kueri Lokasi IP

Waktu update terbaru：2024-01-24 17:48:51

Fitur kueri lokasi IP membantu Anda memperoleh informasi tentang lokasi geografis dan ISP dari alamat IP publik. Misalnya, kueri menunjukkan bahwa alamat IP `123.123.123.123` berada di Beijing dan disediakan oleh China Unicom.

Keterangan:

Saat ini, fitur kueri lokasi IP sedang dalam uji beta. Untuk mencobanya, harap ajukan kelayakan beta.

Fitur ini kini tersedia secara gratis, dan tidak memnyediakan SLA. Fitur akan dikenakan biaya setelah komersialisasi.

Kasus Penggunaan

Anda dapat mengkueri lokasi dan ISP dari alamat IP CVM tujuan dan memilih CVM sumber agar terhubung.

Anda dapat mengkueri lokasi sebenarnya dari IP publik yang Anda beli dari Tencent Cloud atau platform cloud lainnya.

Pembatasan

Saat ini, kueri lokasi IP hanya tersedia untuk alamat IPv4.

Petunjuk

1. Login ke Konsol VPC.
2. Klik **IP and Interface** (IP dan Antarmuka) > **IP Location Query** (Kueri Lokasi IP) di bilah sisi kiri.
3. Masukkan alamat IP untuk kueri, lalu klik

.

Keterangan:

Anda juga dapat memanggil API `DescribeIpGeolocationInfos` atau `DescribeIpGeolocationDatabaseUrl` untuk mengkueri lokasi IP.

Paket Bandwidth

Waktu update terbaru：2024-01-24 17:48:51

Tencent Cloud Bandwidth Package (BWP) adalah metode penagihan agregat multi-IP yang secara signifikan mengurangi biaya akses internet. Ketika instans jaringan publik memiliki puncak lalu lintas pada waktu berbeda, Anda dapat menggunakan BWP untuk penagihan bandwidth agregat untuk menghemat biaya. BWP mendukung penagihan bulanan 5 teratas bulanan dan penagihan persentil bulanan ke-95 untuk kasus penggunaan yang berbeda. BWP membantu Anda mengurangi biaya akses internet dan meningkatkan efisiensi biaya Anda.

Keterangan:

BWP saat ini dalam versi beta. Untuk mencobanya, harap ajukan permohonan.

Untuk operasi BWP umum, lihat

Melihat Bandwidth yang Dapat Ditagih

Menukar Mode Penagihan

Mengelola Paket Bandwidth IP

Mengelola Paket Bandwidth Perangkat

Koneksi Jaringan
NAT Gateway

Waktu update terbaru：2024-01-24 17:48:51

A NAT gateway adalah layanan yang mendukung terjemahan alamat IP dan menyediakan kapabilitas SNAT dan DNAT. Ini dapat menyediakan layanan akses internet yang aman dan berperforma tinggi untuk sumber daya di VPC. Misalnya, layanan ini dapat memberikan jalur keluar yang aman, mengakses jaringan publik untuk beberapa CVM yang belum memiliki akses ke jaringan publik (internet).

Untuk operasi umum NAT gateway, harap lihat:

Memulai

Memodifikasi Konfigurasi NAT Gateway

Mengelola EIP dari NAT Gateway

Mengelola Aturan Penerusan Port

Mengonfigurasi Rute yang Mengarah ke NAT Gateway

VPN Connection

Waktu update terbaru：2024-01-24 17:48:51

Koneksi VPN adalah layanan konektivitas pribadi berdasarkan tunneling jaringan berbasis IPSEC yang menyediakan koneksi Situs ke Situs (Site-to-Site) terenkripsi dan aman antara situs jarak jauh seperti IDC dan sumber daya di Tencent Cloud. Koneksi VPN memungkinkan layanan ini untuk mengakses dan bertukar data rahasia dengan aman melalui infrastruktur jaringan bersama, seperti jaringan publik (internet).
Untuk operasi VPN umum, harap lihat:
VPN Gateway
Gateway Pelanggan
VPN Tunnel
Menghubungkan VPC ke IDC (Perutean Berbasis Kebijakan)
Menghubungkan IDC ke CCN

Direct Connect

Waktu update terbaru：2024-01-24 17:48:52

Direct Connect menghadirkan pendekatan yang cepat dan aman untuk menghubungkan jaringan Tencent Cloud dengan IDC lokal. Layanan ini didasarkan pada saluran khusus TCP/IP Layer 2 yang berakhir pada Direct Connect Gateway berbasis Cloud. Dari sini, Anda dapat mengakses sumber daya Tencent Cloud di berbagai wilayah yang menawarkan lingkungan cloud hibrida yang fleksibel dan andal.

Untuk operasi umum Direct Connection, harap lihat:

Mulai Cepat

Mengelola Koneksi

Mengelola Direct Connect Gateway

Tunnel Khusus

Cloud Connect Network

Waktu update terbaru：2024-01-24 17:48:51

Cloud Connect Network (CCN) adalah layanan konektivitas pribadi global yang dijalankan di backbone jaringan Tencent Cloud. CCN memungkinkan konektivitas antara VPC di semua wilayah, IDC melalui tautan VPN atau Direct Connect dan bahkan penyedia Cloud atau layanan lainnya. Perutean multi-level CCN mampu melakukan pembelajaran mandiri, jadi ketika topologi jaringan berubah, Anda tidak perlu melakukan operasi berbasis jaringan yang membosankan.

Untuk operasi CCN umum, harap lihat:

Interkoneksi Instans Jaringan dalam Satu Akun

Akun Lintas Interkoneksi Instans Jaringan

Pengelolaan Instans

Pengelolaan Rute

Pengelolaan Bandwidth

Manajemen Keamanan
Grup Keamanan
Ikhtisar Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Grup keamanan adalah firewall virtual yang menampilkan pemfilteran paket data stateful. Grup 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 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.

Batas Penggunaan

Untuk informasi selengkapnya tentang batasan dan kuota grup keamanan, harap lihat Ikhtisar Batasan Penggunaan.

Aturan Grup Keamanan

Komponen

Aturan grup keamanan terdiri dari:
Sumber atau tujuan: IP sumber untuk aturan masuk, atau IP tujuan untuk aturan keluar. Ini bisa berupa alamat IP, rentang IP, atau grup keamanan. Untuk informasi selengkapnya, lihat Menambahkan Aturan Grup Keamanan.
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 dulu, 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 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

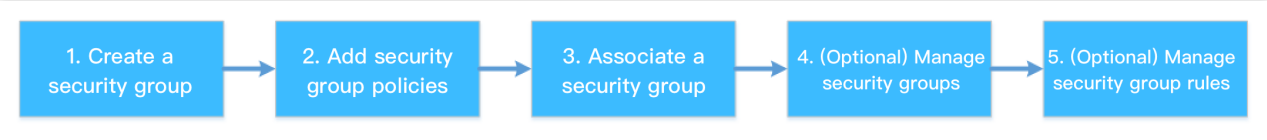
Instans dapat diikat ke satu atau beberapa grup keamanan. Ketika terikat ke beberapa grup keamanan, aturan grup keamanan akan dicocokkan secara berurutan dari atas ke bawah. Anda dapat menyesuaikan prioritas grup keamanan kapan saja.

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 Aplikasi Grup Keamanan.
Jika Anda perlu melindungi lapisan aplikasi (HTTP/HTTPS), harap aktifkan Tencent Cloud Web Application Firewall (WAF) yang memberikan keamanan web pada lapisan aplikasi untuk melindungi dari kerentanan web, perayap berbahaya, dan serangan CC, sehingga melindungi situs web dan keamanan 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, harap gunakan templat parameter.

Mengaitkan grup keamanan

Anda dapat menambahkan instans dengan persyaratan perlindungan yang sama ke grup keamanan yang sama, bukan 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

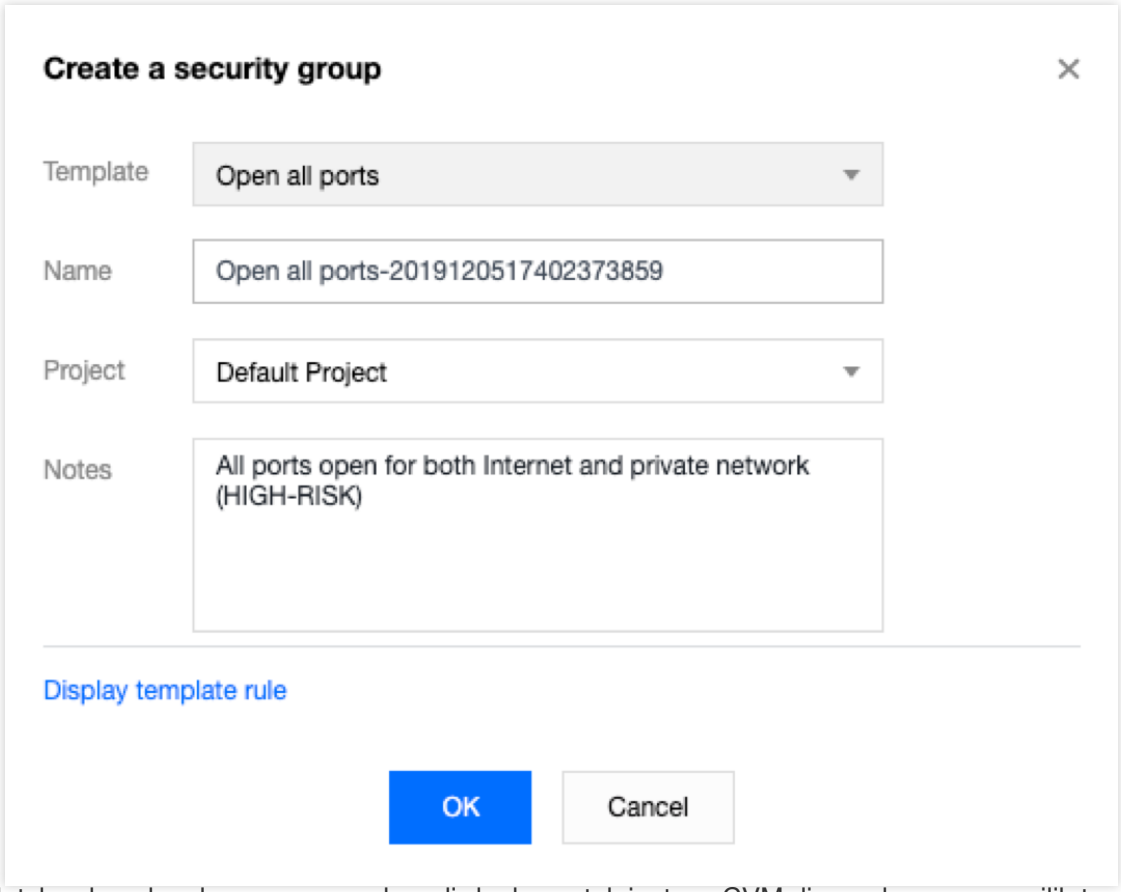
Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Grup keamanan adalah firewall virtual untuk instans CVM. Setiap instans CVM harus dimasukkan dengan setidaknya satu grup keamanan. Tencent Cloud menyediakan dua templat: **Open all ports to the Internet** (Buka semua port ke internet) dan **Open ports 22, 80, 443, and 3389 and ICMP protocol to the Internet** (Buka port 22, 80, 443, dan 3389 serta protokol ICMP ke internet). Dengan templat ini, Anda dapat membuat grup keamanan default saat membuat instans CVM jika belum membuat grup keamanan.
Jika tidak ingin instans CVM bergabung dengan grup keamanan default, Anda dapat membuat grup keamanan lain di konsol CVM sebagai berikut:

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah) dan klik **+Create** (+Buat).
4. Pada jendela **Create a security group** (Buat grup keamanan) yang muncul, selesaikan konfigurasi seperti yang ditunjukkan pada gambar berikut:



Templat: berdasarkan layanan yang akan di-deploy untuk instans CVM di grup keamanan, pilih templat yang sesuai untuk menyederhanakan konfigurasi aturan grup keamanan seperti yang dijelaskan dalam tabel berikut:

Templat	Deskripsi	Skenario
Buka semua port ke internet	Secara default, semua port akan dibuka ke internet dan jaringan pribadi yang kemudian dapat menimbulkan risiko keamanan.	-
Buka port 22, 80, 443, dan 3389 dan protokol ICMP ke internet	Secara default, port 22, 80, 443, dan 3389 dan protokol ICMP akan dibuka ke internet. Selain itu, semua port akan dibuka ke jaringan pribadi.	Layanan web perlu di-deploy untuk instans dalam grup keamanan.
Kustom	Setelah membuat grup keamanan, Anda dapat menambahkan aturan grup keamanan sesuai kebutuhan. Untuk detail tentang operasi, lihat Menambahkan Aturan Grup Keamanan.	-

Nama: menyesuaikan nama grup keamanan.

Proyek: secara default, **Default project** (Proyek default) dipilih. Anda juga dapat menentukan proyek lain untuk memfasilitasi manajemen di masa mendatang.

Keterangan: jelaskan grup keamanan secara singkat untuk memfasilitasi manajemen di masa mendatang.

5. Klik **OK** (Oke) untuk menyelesaikan pembuatan grup keamanan.
Jika Anda memilih templat **Custom** (Kustom) saat membuat grup keamanan, klik **Set rules now** (Tetapkan aturan sekarang) setelah pembuatan ke tambahkan aturan grup keamanan.

Menambahkan Aturan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Grup keamanan digunakan untuk menentukan apakah akan mengizinkan permintaan akses dari internet atau jaringan pribadi. Untuk pertimbangan keamanan, penolakan akses digunakan di arah masuk dalam banyak kasus. Jika Anda memilih templat "Buka semua port ke internet" atau "Buka port 22, 80, 443, dan 3389 dan protokol ICMP ke internet" saat membuat grup keamanan, sistem akan secara otomatis menambahkan aturan grup keamanan untuk beberapa port komunikasi berdasarkan templat yang dipilih.
Dokumen ini menjelaskan cara menambahkan aturan grup keamanan guna mengizinkan atau melarang CVM dalam grup keamanan untuk mengakses internet atau instans VPC.

Catatan

Aturan grup keamanan dibagi menjadi aturan grup keamanan IPv4 dan IPv6.
Open all ports (Buka semua port) berlaku untuk aturan grup keamanan IPv4 dan IPv6.

Prasyarat

Anda telah membuat grup keamanan.
Anda mengetahui permintaan akses internet atau jaringan pribadi yang perlu diizinkan atau ditolak untuk instans CVM Anda. - Untuk kasus penggunaan lainnya dari pengaturan aturan grup keamanan, lihat Kasus Penggunaan Grup Keamanan.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan baris grup keamanan yang ingin Anda tetapkan aturannya.
4. Di kolom operasi, klik **Modify Rules** (Modifikasi Aturan).
5. Pa
da halama

n aturan grup keamanan, klik **Inbound rules** (Aturan masuk), dan pilih salah satu mode berikut berdasarkan kebutuhan aktual Anda untuk menyelesaikan operasi.

Keterangan:

Contoh operasi berikut menggunakan mode 2 (aturan penambahan).

Mode 1 (buka semua port): berlaku untuk skenario dengan aturan protokol ICMP yang tidak perlu diatur dan operasi yang dapat dilakukan melalui port 22, 3389, 80, 443, 20, dan 21, serta protokol ICMP .

Mode 2 (aturan penambahan): berlaku untuk skenario dengan beberapa protokol komunikasi, seperti ICMP yang perlu diatur.

6. Pada jendela **Add Inbound Rules** (Tambahkan Aturan Masuk) yang muncul, tetapkan aturan.

Parameter utama yang diperlukan untuk menambahkan aturan adalah sebagai berikut:

Ketik: nilai default adalah "Custom" (Kustom). Anda juga dapat memilih templat aturan sistem lain, seperti "Login Windows", "Login Linux", "Ping", "HTTP (80)", atau "HTTPS (443)".

Sumber/Tujuan: sumber (aturan masuk) atau tujuan (aturan keluar) lalu lintas. Pilih salah satu opsi berikut:

Sumber/Tujuan Tertentu	Deskripsi
Alamat IPv4 atau rentang alamat IPv4	Tentukan dalam notasi CIDR (misalnya, 203.0.113.0, 203.0.113.0/24, atau 0.0.0.0/0, di mana 0.0.0.0/0 menunjukkan bahwa semua alamat IPv4 akan dicocokkan).
Alamat IPv6 atau rentang alamat IPv6	Tentukan dalam notasi CIDR (misalnya, FF05::B5, FF05:B5::/60, ::/0, or 0::0/0, di mana ::/0 atau 0::0/0 menunjukkan bahwa semua alamat IPv6 akan dicocokkan).
Impor ID grup keamanan: Anda dapat mengimpor ID grup keamanan berikut: ID grup keamanan Grup keamanan lain	Grup keamanan saat ini mengacu pada CVM yang terhubung ke grup keamanan. Grup keamanan lain mengacu pada ID grup keamanan lain di proyek yang sama di wilayah yang sama.
Impor objek alamat IP atau objek grup alamat IP di templat parameter.	-

Port protokol: masukkan jenis protokol dan rentang port, atau impor port protokol atau grup port protokol di templat parameter.

Kebijakan: nilai defaultnya adalah "Permit" (Izinkan).

Permit (Izinkan): mengizinkan permintaan akses melalui port.

Reject (Tolak): menghapus paket data secara langsung tanpa mengembalikan respons apa pun.

Remarks (Keterangan): menjelaskan secara singkat aturan untuk memfasilitasi pengelolaan di masa mendatang.

7. Klik **F**

inish (S
elesai). Aturan masuk ditambahkan ke grup keamanan.
8. Pada halaman aturan grup keamanan, klik **Outbound Rules** (Aturan Keluar), dan tambahkan aturan keluar ke grup keamanan dengan merujuk ke Langkah 5 ke Langkah 7.

Menghubungkan Instans CVM dengan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Sebagai metode isolasi keamanan jaringan yang penting, grup keamanan digunakan untuk mengonfigurasi kontrol akses jaringan untuk satu atau lebih CVM. Anda dapat menghubungkan instans CVM dengan satu atau beberapa grup keamanan berdasarkan kebutuhan bisnis Anda. Dokumen ini menjelaskan cara menghubungkan instans CVM dengan grup keamanan di konsol.

Prasyarat

Instans CVM telah dibuat.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan baris grup keamanan yang ingin Anda tetapkan aturannya.
4. Di kolom operasi, klik **Manage instance** (Kelola instans) untuk masuk ke halaman **Associate with Instance** (Hubungkan ke Instans).
5. Di halaman **Associate with Instance** (Hubungkan ke Instans), klik **Add Association** (Tambahkan Hubungan).
6. Di jendela "Add Instance Association" (Tambahkan Hubungan Instans) yang muncul, pilih instans yang akan dihubungkan dengan grup keamanan dan klik **OK** (Oke).

Operasi Selanjutnya

Untuk melihat semua grup keamanan yang telah dibuat di suatu wilayah, mengkueri daftar grup keamanan.
Untuk detail tentang operasi, lihat Melihat Grup Keamanan.
Jika Anda tidak ingin instans CVM menjadi bagian dari satu atau beberapa grup keamanan, hapus instans dari grup tersebut.

Untuk detail tentang operasi, lihat Menghapus dari Grup Keamanan.

Jika bisnis tidak lagi membutuhkan satu atau beberapa grup keamanan, Anda dapat menghapusnya. Setelah Anda menghapus grup keamanan, semua aturan grup keamanan di dalamnya juga akan dihapus.

Untuk detail tentang operasi, lihat Menghapus Grup Keamanan.

Mengelola Grup Keamanan

Melihat Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Untuk melihat semua grup keamanan yang telah Anda buat di wilayah tertentu, selesaikan langkah-langkah berikut.

Langkah

Melihat semua grup keamanan

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), lalu Anda dapat melihat semua grup keamanan di wilayah tersebut.

Melihat grup keamanan tertentu

Anda dapat menggunakan fitur pencarian di halaman manajemen grup keamanan untuk melihat grup keamanan tertentu.

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Di halaman manajemen grup keamanan, pilih **Region** (Wilayah).
4. Di sudut kanan atas daftar grup keamanan wilayah, klik kotak teks pencarian, dan pilih salah satu metode berikut untuk mengkueri grup keamanan target.

Pilih **Security Group ID** (ID Grup Keamanan), masukkan ID grup keamanan, dan klik

untuk mengkueri grup keamanan terkait.

Pilih **Security Group Name** (Nama Grup Keamanan), masukkan nama grup keamanan, dan klik

untuk mengkueri grup keamanan terkait.

Pilih **Label**, masukkan nama label, dan klik

untuk mengkueri semua grup keamanan dengan label.

Operasi Lainnya

Untuk mempelajari selengkapnya tentang sintaksis guna melihat grup keamanan tertentu, klik

di kotak teks pencarian untuk melihat sintaksis yang relevan.

Menghapus dari Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Anda dapat menghapus instans CVM dari grup keamanan berdasarkan kebutuhan bisnis Anda.

Prasyarat

Instans CVM yang akan dihapus telah bergabung dengan dua atau beberapa grup keamanan.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan baris grup keamanan tempat instans ingin dihapus.
4. Di kolom operasi, klik **Manage instances** (Kelola instans) untuk masuk ke halaman **Associate with Instance** (Hubungkan ke Instans).
5. Pada halaman **Associate with Instance** (Hubungkan ke Instans), pilih instans yang akan dihapus dan klik **Remove from security group** (Hapus dari grup keamanan).
6. Di jendela yang muncul, klik **OK** (OKE).

Mengkloning Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Anda mungkin perlu mengkloning grup keamanan dalam skenario berikut:
Anda telah membuat grup keamanan bernama sg-A di wilayah A dan ingin menerapkan aturan sg-A ke instans di wilayah B. Dalam hal ini, Anda dapat mengkloning sg-A ke wilayah B alih-alih membuat grup keamanan lain di wilayah B.
Bisnis Anda perlu menjalankan aturan grup keamanan baru. Dalam hal ini, Anda dapat mengkloning grup keamanan asli untuk cadangan.

Catatan

Secara default, hanya aturan masuk dan keluar dari grup keamanan yang dikloning, tetapi bukan instans yang terhubung ke grup keamanan.
Grup keamanan dapat dikloning antar proyek atau wilayah.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah) dan temukan baris grup keamanan yang akan dikloning.
4. Di kolom operasi, klik **More** (Lainnya) > **Clone** (Kloning).
5. Di jendela "Clone Security Group" (Kloning Grup Keamanan" yang muncul, pilih **Target Project** (Proyek Target) dan **Target Region** (Wilayah Target) untuk kloning, masukkan **New Name** (Nama Baru) untuk grup keamanan, dan klik **OK** (Oke).

Menghapus Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Jika bisnis tidak lagi memerlukan satu atau beberapa grup keamanan, Anda dapat menghapusnya. Setelah menghapus grup keamanan, semua aturan grup keamanan di grup juga akan dihapus.

Prasyarat

Grup keamanan yang akan dihapus tidak terhubung ke instans apa pun. Jika terhubung ke instans, hapus grup dari grup keamanan terlebih dahulu. Jika tidak, grup keamanan tidak dapat dihapus. Untuk detail tentang operasi, lihat Menghapus dari Grup Keamanan.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan baris grup keamanan yang akan dihapus.
4. Di kolom operasi, klik **More** (Lainnya) > **Delete** (Hapus).
5. Di jendela yang muncul, klik **OK** (OKE).

Menyesuaikan Prioritas Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Ikhtisar

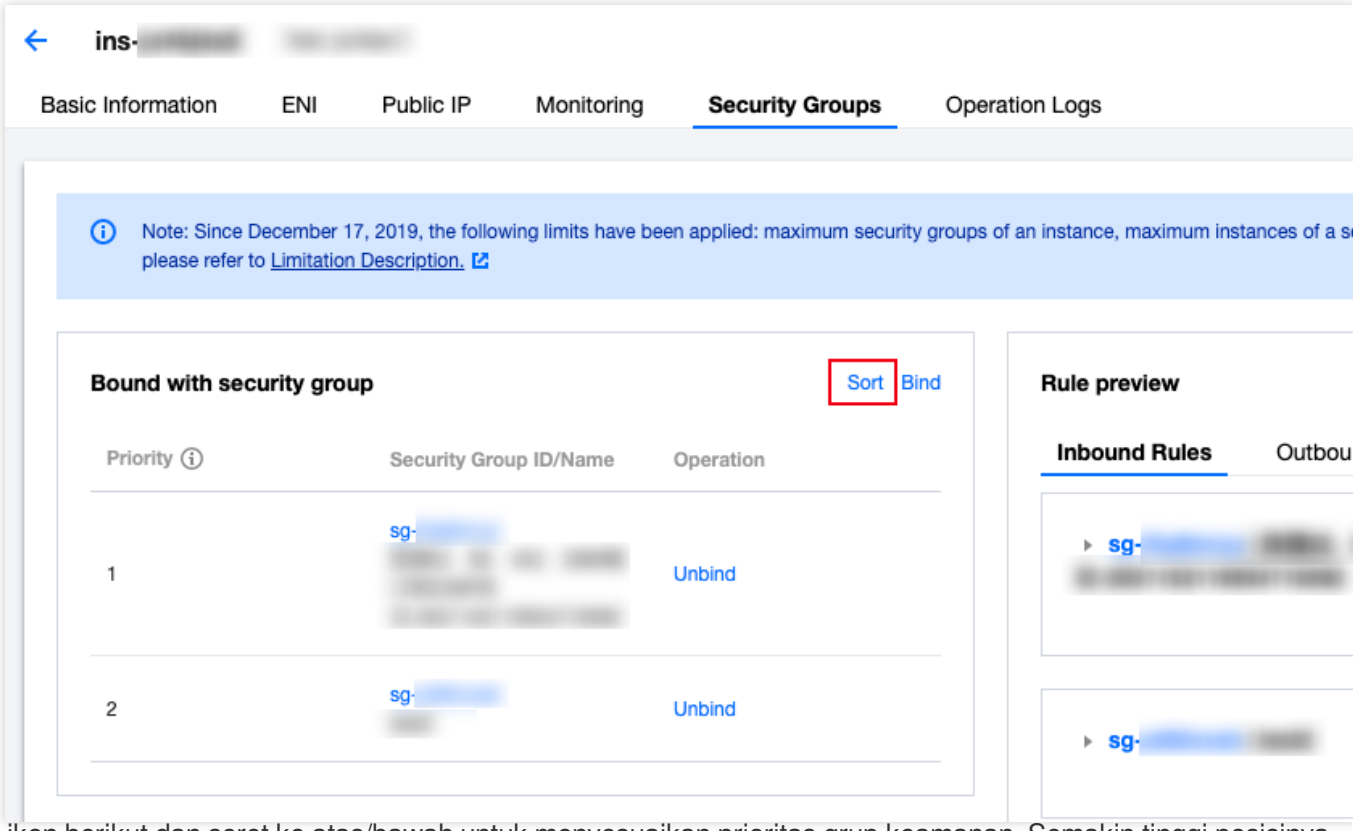
Anda dapat mengikat satu atau beberapa grup keamanan ke CVM. Jika Anda telah mengikat beberapa grup keamanan, grup keamanan ini dijalankan berdasarkan prioritasnya. Anda dapat menyesuaikan prioritas sebagai berikut.

Prasyarat

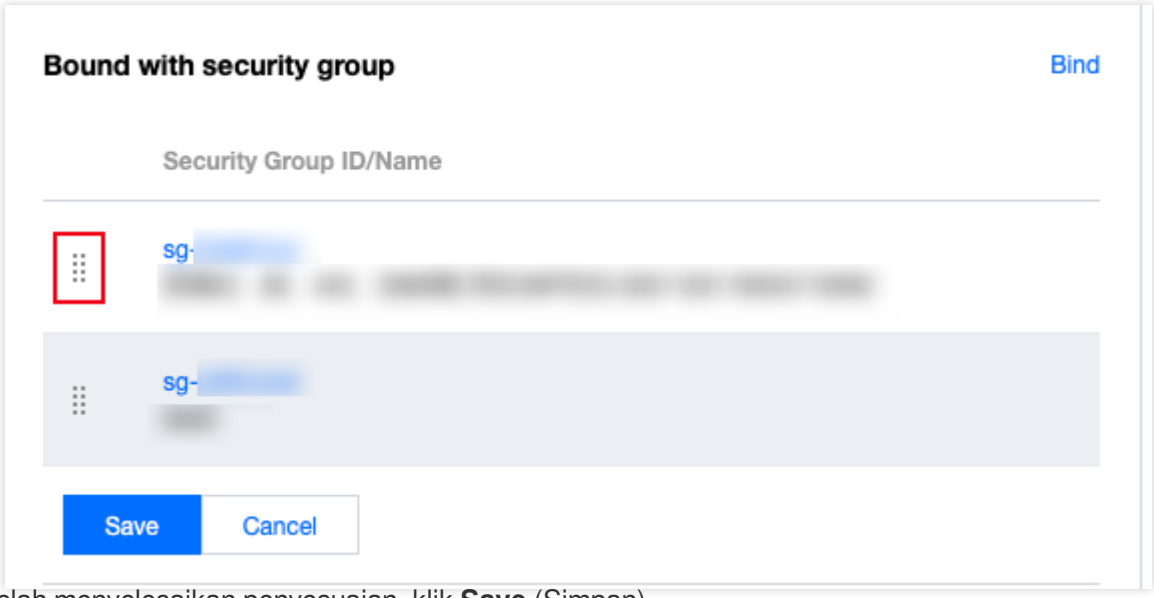
Instans CVM terikat ke dua atau beberapa grup keamanan.

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. Pada modul **Bound Security Groups** (Grup Keamanan Terikat), klik **Sort** (Urutkan).



5. Klik ikon berikut dan seret ke atas/bawah untuk menyesuaikan prioritas grup keamanan. Semakin tinggi posisinya, semakin tinggi tingkat prioritas grup keamanan.



6. Setelah menyelesaikan penyesuaian, klik **Save** (Simpan).

Mengelola Aturan Grup Keamanan
Melihat Aturan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Setelah menambahkan aturan grup keamanan, Anda dapat melihat detailnya di konsol.

Prasyarat

Anda telah membuat grup keamanan dan menambahkan aturan grup keamanan ke grup.
Untuk informasi selengkapnya tentang cara membuat grup keamanan dan menambahkan aturan grup keamanan, lihat Menambahkan Grup Keamanan.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan grup keamanan dengan aturan yang ingin dilihat.
4. Klik ID atau nama grup keamanan target untuk masuk ke halaman aturan grup keamanan.
5. Pada halaman aturan grup keamanan, klik tab **Inbound Rules or Outbound Rules** (Aturan Masuk atau Aturan Keluar) untuk melihat aturan masuk atau keluar grup keamanan.

Memodifikasi Aturan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Aturan grup keamanan yang tidak ditetapkan dengan benar (misalnya, aturan yang tidak membatasi akses ke port tertentu) dapat menimbulkan risiko keamanan yang serius. Dalam hal ini, Anda dapat mengubah aturan grup keamanan ini dalam grup keamanan untuk memastikan keamanan jaringan instans CVM. Dokumen ini menjelaskan cara mengubah aturan grup keamanan.

Prasyarat

Anda telah membuat grup keamanan dan menambahkan aturan grup keamanan ke grup.
Untuk informasi selengkapnya tentang cara membuat grup keamanan dan menambahkan aturan grup, lihat Menambahkan Aturan Grup Keamanan.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan baris grup keamanan yang aturannya akan diubah.
4. Di kolom operasi, klik **Modify Rules** (Modifikasi Aturan) untuk masuk ke halaman aturan grup keamanan.
5. Pada halaman aturan grup keamanan, klik tab **Inbound Rules or Outbound Rules** (Aturan Masuk atau Aturan Keluar) berdasarkan arah (masuk atau keluar) aturan grup keamanan yang akan diubah.
6. Temukan aturan grup keamanan yang ingin diubah dan klik **Edit** di kolom operasi untuk mengubahnya.

Menghapus Aturan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Jika tidak lagi memerlukan aturan grup keamanan, Anda dapat menghapusnya.

Prasyarat

Anda telah membuat grup keamanan dan menambahkan aturan grup keamanan ke grup.
Untuk informasi selengkapnya tentang cara menyetel aturan grup keamanan, lihat Menambahkan Aturan Grup Keamanan.
Anda telah mengonfirmasi bahwa instans CVM tidak perlu mengizinkan atau melarang akses internet atau akses jaringan pribadi.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan baris grup keamanan dengan aturan yang akan dihapus.
4. Di kolom operasi, klik **Modify Rules** (Modifikasi Aturan) untuk masuk ke halaman aturan grup keamanan.
5. Pada halaman aturan grup keamanan, klik tab **Inbound Rules or Outbound Rules** (Aturan Masuk atau Aturan Keluar) berdasarkan arah (masuk atau keluar) aturan grup keamanan yang akan dihapus.
6. Temukan aturan grup keamanan yang ingin Anda hapus dan klik **Delete** (Hapus).
7. Di jendela pop-up, klik **OK** (OKE).

Mengimpor Aturan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Anda dapat mengimpor file aturan grup keamanan yang diekspor ke grup keamanan untuk membuat atau memulihkan aturan grup keamanan dengan cepat.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan grup keamanan dengan aturan yang ingin diimpor.
4. Klik ID atau nama grup keamanan untuk masuk ke halaman aturan grup keamanan.
5. Pada halaman aturan grup keamanan, klik tab **Inbound Rules or Inbound Rules** (Aturan Masuk atau Keluar) berdasarkan arah (masuk atau keluar) aturan grup keamanan yang akan diimpor.
6. Pada halaman tab **Inbound Rules or Inbound Rules** (Aturan Masuk atau Aturan Keluar) , klik **Import Rules** (Impor Aturan).
7. Pada jendela **Batch Import-Inbound/Outbound Rules** (Impor Batch-Aturan Masuk/Keluar) yang muncul, pilih file aturan masuk atau keluar templat yang telah diedit dan klik **Import** (Impor).

Keterangan:

Jika aturan grup keamanan sudah ada di grup keamanan tempat aturan akan diimpor, sebaiknya mengekspor aturan ini terlebih dahulu. Jika tidak, aturan yang diimpor akan menimpa yang sudah ada.

Jika tidak ada aturan grup keamanan di grup keamanan tempat aturan akan diimpor, sebaiknya mengunduh file templat terlebih dahulu, mengedit file templat, lalu mengimpor file.

Mengekspor Aturan Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Skenario Operasi

Anda dapat mengekspor aturan grup keamanan dari grup keamanan untuk cadangan lokal.

Langkah

1. Login ke konsol CVM.
2. Di bilah sisi kiri, klik **Security Group** (Grup Keamanan) untuk masuk ke halaman manajemen grup keamanan.
3. Pada halaman manajemen grup keamanan, pilih **Region** (Wilayah), dan temukan grup keamanan dengan aturan yang akan diekspor.
4. Klik ID atau nama grup keamanan untuk masuk ke halaman aturan grup keamanan.
5. Pada halaman aturan grup keamanan, klik tab **Inbound Rules or Outbound Rules** (Aturan Masuk atau Aturan Keluar) berdasarkan arah (masuk atau keluar) aturan grup keamanan yang akan diekspor.
6. Pada halaman tab **Inbound Rules or Outbound Rules** (Aturan Masuk atau Aturan Keluar), klik

di sudut kanan atas untuk mengunduh dan menyimpan file aturan grup keamanan ke direktori lokal.

Kasus Aplikasi Grup Keamanan

Waktu update terbaru：2024-01-24 17:55:51

Grup keamanan digunakan untuk mengelola apakah Cloud Virtual Machine (CVM) dapat diakses. 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:
Untuk memastikan keamanan data, aturan masuk untuk grup keamanan adalah kebijakan penolakan yang menolak akses jarak jauh dari jaringan eksternal. Agar CVM dapat diakses oleh sumber daya eksternal, Anda harus mengizinkan aturan masuk untuk port yang sesuai.
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 ICMP** (Buka Port 22, 80, 443, dan 3389 dan ICMP), aturan keluar untuk grup keamanan akan membuka port ke internet. Jika Anda memilih aturan grup keamanan kustom, aturan keluar akan memblokir semua port secara default, dan Anda perlu menetapkan aturan keluar untuk mengizinkan port terkait mengakses sumber daya jaringan eksternal.

Kasus Penggunaan Umum

Dokumen ini menjelaskan beberapa kasus penggunaan umum untuk grup keamanan. Jika salah satu kasus berikut memenuhi persyaratan Anda, Anda dapat mengatur grup keamanan Anda sesuai dengan konfigurasi yang direkomendasikan untuk kasus penggunaan yang sesuai.

Skenario 1: menghubungkan CVM Linux dari jarak jauh melalui SSH

Case (Kasus): Anda telah membuat CVM Linux dan ingin terhubung ke CVM dari jarak jauh melalui SSH.
Solution (Solusi): saat menambahkan aturan masuk, atur **Type** (Jenis) ke **Linux Login** (Login Linux) dan buka port TCP 22 ke internet untuk mengizinkan login Linux melalui SSH.
Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang alamat IP) ke internet sesuai kebutuhan. Tindakan ini mengizinkan Anda untuk mengonfigurasi alamat IP sumber yang dapat mengakses CVM dari jarak jauh melalui SSH.

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Login Linux	Semua alamat IP: 0.0.0.0/0 Alamat IP yang ditentukan: alamat IP atau rentang alamat IP tertentu	TCP: 22	Izinkan

Skenario 2: menghubungkan dari jarak jauh ke Windows CVM melalui RDP

Case (Kasus): Anda telah membuat CVM Windows dan ingin terhubung ke CVM dari jarak jauh melalui Koneksi Desktop Jarak Jauh (RDP).
Solution (Solusi): saat menambahkan aturan masuk, atur **Type** (Jenis) ke **Windows Login** (Login Windows) 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 alamat IP) ke internet sesuai kebutuhan. Ini mengizinkan Anda untuk mengonfigurasi alamat IP sumber yang dapat mengakses CVM dari jarak jauh melalui RDP.

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Login Windows	Semua alamat IP: 0.0.0.0/0 Alamat IP yang ditentukan: alamat IP atau rentang alamat IP tertentu	TCP: 3389	Izinkan

Skenario 3: melakukan ping CVM dari internet

Case (Kasus): Anda telah membuat CVM dan ingin memeriksa apakah komunikasi antara CVM dan CVM lain normal.
Solution (Solusi): uji koneksi dengan menggunakan program ping. Khususnya, saat menambahkan aturan masuk, atur **Type** (Jenis) ke **Ping** (Ping) dan buka port Internet Control Message Protocol (ICMP) ke internet untuk memungkinkan CVM lain mendapatkan akses ke CVM ini melalui ICMP.
Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang alamat IP) ke internet sesuai kebutuhan. Tindakan ini memungkinkan Anda untuk mengonfigurasi alamat IP sumber yang dapat mengakses CVM ini melalui ICMP.

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Ping	Semua alamat IP: 0.0.0.0/0 Alamat IP tertentu: alamat IP atau rentang alamat tertentu	ICMP	Izinkan

Skenario 4: login jarak jauh ke CVM melalui Telnet

Case (Kasus): Anda ingin login jarak jauh ke CVM melalui Telnet.
Solution (Solusi): saat menambahkan aturan masuk, konfigurasi aturan grup keamanan berikut:

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Kustom	Semua alamat IP: 0.0.0.0/0 Alamat IP yang ditentukan: alamat IP atau rentang alamat IP tertentu	TCP: 23	Izinkan

Skenario 5: mengotorisasi akses ke layanan web melalui HTTP atau HTTPS

Case (Kasus): Anda telah membuat situs web dan ingin mengizinkan pengguna mengakses situs web Anda melalui HTTP atau HTTPS.

Solution (Solusi): saat menambahkan aturan masuk, konfigurasi aturan grup keamanan berikut sesuai kebutuhan:

Izinkan semua alamat IP di internet untuk mengakses situs web ini

Arah	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 di internet untuk mengakses situs web ini

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	HTTP (80)	Alamat IP atau rentang alamat IP yang diizinkan untuk mengakses situs web Anda	TCP: 80	Izinkan
Masuk	HTTPS (443)	Alamat IP atau rentang alamat 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 tertentu (seperti port 1101) dapat diakses secara eksternal.

Solution (Solusi): saat menambahkan aturan masuk, atur **Type** (Jenis) ke **Custom** (Kustom) dan buka port TCP 1101 ke internet untuk mengizinkan sumber daya eksternal mengakses port layanan tertentu.

Anda dapat membuka semua alamat IP atau alamat IP tertentu (atau rentang alamat IP) ke internet sesuai kebutuhan. Tindakan ini memungkinkan alamat IP sumber untuk mengakses port layanan tertentu.

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Kustom	Semua alamat IP: 0.0.0.0/0 Alamat IP yang ditentukan: alamat IP atau rentang alamat IP tertentu	TCP: 1101	Izinkan

Skenario 7: menolak akses ke port tertentu dari alamat IP eksternal

Case (Kasus): Anda telah men-deploy layanan dan ingin memblokir akses eksternal ke port layanan tertentu (seperti port 1102).

Solution (Solusi): saat menambahkan aturan masuk, atur **Type** (Jenis) ke **Custom** (Kustom), konfigurasi port TCP 1102, dan atur **Policy** (Kebijakan) ke **Reject** (Tolak) untuk menolak akses eksternal ke port layanan tertentu.

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Kustom	Semua alamat IP: 0.0.0.0/0 Alamat IP yang ditentukan: alamat IP atau rentang alamat IP tertentu	TCP: 1102	Tolak

Skenario 8: mengizinkan CVM hanya mengakses 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 dengan mengacu pada konfigurasi berikut:

Izinkan instans CVM mengakses alamat IP publik tertentu

Larang instans CVM mengakses alamat IP publik apa pun melalui protokol apa pun

Keterangan:

Aturan yang mengizinkan akses harus memiliki prioritas lebih tinggi dari aturan yang menolak akses.

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Keluar	Kustom	Alamat IP publik tertentu yang dapat diakses oleh CVM	Protokol dan port yang diperlukan	Izinkan
Keluar	Kustom	0.0.0.0/0	Semua	Tolak

Skenario 9: menolak 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 dengan mengacu pada konfigurasi berikut:

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Keluar	Kustom	Alamat IP publik tertentu yang tidak ingin diakses oleh CVM	Semua	Tolak

Skenario 10: mengunggah file ke atau mengunduh file dari CVM melalui FTP

Case (Kasus): Anda ingin mengunggah file ke atau mengunduh file dari CVM dengan menggunakan program FTP.

Solution (Solusi): tambahkan aturan grup keamanan dengan mengacu pada konfigurasi berikut:

Arah	Jenis	Sumber	Port Protokol	Kebijakan
Masuk	Kustom	0.0.0.0/0	TCP: 20-21	Izinkan

Kombinasi Beberapa Skenario

Dalam skenario aktual, Anda mungkin ingin mengonfigurasi beberapa aturan grup keamanan berdasarkan persyaratan layanan, misalnya, mengonfigurasi aturan masuk atau keluar secara bersamaan. Satu CVM mungkin terikat ke satu atau lebih grup keamanan. Ketika CVM terikat ke beberapa grup keamanan, grup keamanan ini dicocokkan dan dijalankan dalam urutan prioritas yang menurun. Anda dapat menyesuaikan prioritas grup keamanan ini kapan pun diperlukan.

Port Server Umum

Waktu update terbaru：2024-01-24 17:55:51

Berikut ini menjelaskan port server umum. Untuk informasi selengkapnya tentang port aplikasi layanan untuk Windows, lihat dokumen resmi Microsoft (Ikhtisar Layanan Windows dan Persyaratan Port Jaringan).

Nomor Port	Layanan	Deskripsi
21	FTP	Port server FTP terbuka untuk mengunggah dan mengunduh.
22	SSH	Port 22 adalah port SSH. Ini digunakan untuk terhubung dari jarak jauh ke server Linux dalam mode CLI.
25	SMTP	Port terbuka server SMTP untuk mengirim email.
80	HTTP	Port ini digunakan untuk layanan web seperti IIS, Apache, dan Nginx untuk menyediakan akses eksternal.
110	POP3	Port 110 terbuka 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 melalui port 139 mencoba mengakses layanan NetBIOS/SMB. Protokol ini digunakan untuk berbagi file dan printer di Windows dan SAMBA.
143	IMAP	Port 143 utamanya digunakan untuk Internet Message Access Protocol (IMAP) v2, protokol untuk menerima email yang serupa dengan POP3.
443	HTTPS	Port penelusuran web. HTTPS adalah jenis HTTP lain yang menyediakan enkripsi dan transmisi melalui port aman.
1433	SQL Server	Port 1433 adalah port default untuk SQL Server. SQL Server menggunakan dua port: port 1433 untuk TCP dan port 1434 untuk UDP. Port 1433 digunakan untuk SQL Server untuk menyediakan layanan eksternal, sedangkan port 1434 digunakan untuk menanggapi pemohon mengenai port TCP/IP yang digunakan oleh SQL Server.
3306	MySQL	Port 3306 adalah port default untuk database MySQL dan digunakan untuk menyediakan layanan eksternal.
3389	Windows Server Remote Desktop Services	Port 3389 adalah port untuk layanan desktop jarak jauh di Windows 2000/2003 Server yang memungkinkan Anda terhubung ke server jauh menggunakan alat sambungan Desktop Jarak Jauh.

8080	Port proksi	Mirip dengan port 80, port 8080 digunakan untuk layanan proksi WWW untuk penjelajahan web. Ekstensi nomor port ":8080" sering ditambahkan ke URL saat pengguna mengunjungi situs web atau menggunakan server proksi. Selain itu, setelah server web Apache Tomcat diinstal, port layanan defaultnya adalah port 8080.

ACL Jaringan

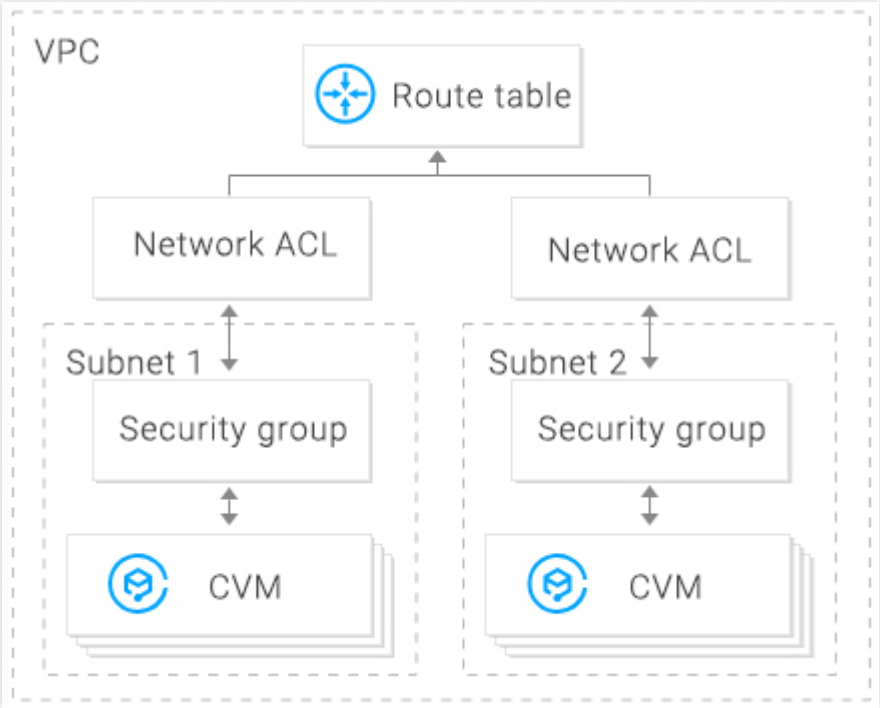
Ikhtisar Aturan

Waktu update terbaru：2024-01-24 17:55:51

Network Access Control List (ACL) adalah lapisan keamanan opsional yang membatasi lalu lintas ke dan dari subnet yang akurat ke protokol dan port.

Ikhtisar

Anda dapat menghubungkan ACL jaringan dengan beberapa subnet untuk mempertahankan lalu lintas yang sama dan mengontrol arus masuk dan keluarnya secara tepat dengan menetapkan aturan masuk dan keluar.
Misalnya, saat menghosting aplikasi web multi-lapisan di instans Tencent Cloud VPC dan membuat subnet yang berbeda untuk layanan lapisan web, lapisan logis, dan lapisan data, Anda dapat menggunakan ACL jaringan untuk memastikan bahwa lapisan web dan subnet lapisan data tidak dapat mengakses satu sama lain, tetapi hanya subnet lapisan logis yang dapat mengakses subnet lapisan web dan lapisan data.



Aturan ACL

Saat aturan ACL jaringan ditambahkan atau dihapus, perubahan akan diterapkan ke subnet terhubung secara otomatis.
Anda dapat mengonfigurasi aturan ACL jaringan masuk dan keluar. Setiap aturan terdiri dari:
IP Sumber/IP tujuan: masukkan IP sumber untuk aturan masuk atau IP tujuan untuk aturan keluar. Format yang didukung:
IP tunggal: seperti “192.168.0.1” atau “FF05::B5”
Blok CIDR: seperti “192.168.1.0/24” atau “FF05:B5::/60”
Semua alamat IPv4: “0.0.0.0/0”
Jenis protokol: menunjukkan jenis protokol yang diizinkan atau ditolak oleh aturan ACL, misalnya, TCP dan UDP.
Port: menunjukkan port sumber atau tujuan lalu lintas. Format yang didukung:
Port tunggal: seperti "22" atau "80"
Rentang port: seperti "1-65535" atau "100-20000"
Semua port: Semua
Kebijakan: menunjukkan apakah akan mengizinkan atau menolak permintaan akses.

Aturan default

Setelah dibuat, setiap ACL jaringan memiliki dua aturan default yang tidak dapat diubah atau dihapus, dengan prioritas terendah.
Aturan masuk default

Jenis Protokol	Port	Sumber IP	Kebijakan	Deskripsi
Semua	Semua	0.0.0.0/0	Tolak	Menolak semua lalu lintas masuk.

Aturan keluar default

Jenis Protokol	Port	IP tujuan	Kebijakan	Deskripsi
Semua	Semua	0.0.0.0/0	Tolak	Menolak semua lalu lintas keluar.

Prioritas aturan

Aturan jaringan ACL diprioritaskan dari atas ke bawah. Aturan di bagian atas daftar memiliki prioritas tertinggi dan akan berlaku lebih dulu, 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.
Ketika lalu lintas masuk atau keluar dari subnet yang terikat ke jaringan ACL, aturan ACL jaringan akan dicocokkan secara berurutan dari atas ke bawah. Jika aturan berhasil dicocokkan dan berlaku, aturan berikutnya tidak akan cocok.

Contoh aplikasi

Untuk mengizinkan semua alamat IP sumber mengakses semua port CVM di subnet yang terhubung ke ACL jaringan dan menolak alamat IP sumber HTTP `192.168.200.11/24` untuk mengakses port 80, tambahkan dua aturan ACL jaringan berikut untuk lalu lintas masuk:

Jenis Protokol	Port	IP Sumber	Kebijakan	Deskripsi
HTTP	80	192.168.200.11/24	Tolak	Menolak alamat IP layanan HTTP ini untuk mengakses port 80.
Semua	Semua	0.0.0.0/0	Izinkan	Mengizinkan semua alamat IP sumber mengakses semua port.

Grup Keamanan vs. ACL Jaringan

Item	Grup Keamanan	Jaringan ACL
Pelambatan lalu lintas	Pelambatan lalu lintas di tingkat instans, seperti CVM dan database	Pelambatan lalu lintas di tingkat subnet
Aturan	Aturan izinkan dan tolak	Aturan izinkan dan tolak
Stateful atau stateless	Stateful: lalu lintas yang dikembalikan secara otomatis diizinkan tanpa tunduk pada aturan apa pun.	Stateless: lalu lintas yang dikembalikan harus secara eksplisit diizinkan oleh aturan.
Waktu efektif	Aturan diterapkan ke instans, seperti CVM atau TencentDB,kecuali Anda menentukan grup keamanan saat membuat instans atau menghubungkan grup keamanan ke instans setelah dibuat.	Aturan ACL diterapkan secara otomatis ke semua instans, seperti instans CVM dan TencentDB di subnet terhubung.
Prioritas aturan	Jika terjadi konflik aturan, aturan dengan prioritas lebih tinggi akan berlaku secara default.	Jika terjadi konflik aturan, aturan dengan prioritas lebih tinggi akan berlaku secara default.

Batasan

Waktu update terbaru：2024-01-24 17:55:51

Batasan Penggunaan

Satu jaringan ACL dapat diikatkan ke beberapa subnet.
ACL jaringan bersifat stateless. Dengan demikian, Anda perlu menetapkan masing-masing aturan keluar dan aturan masuk.
ACL jaringan tidak memengaruhi interkomunikasi jaringan pribadi antar instans CVM di subnet terhubung.

Batasan Kuota

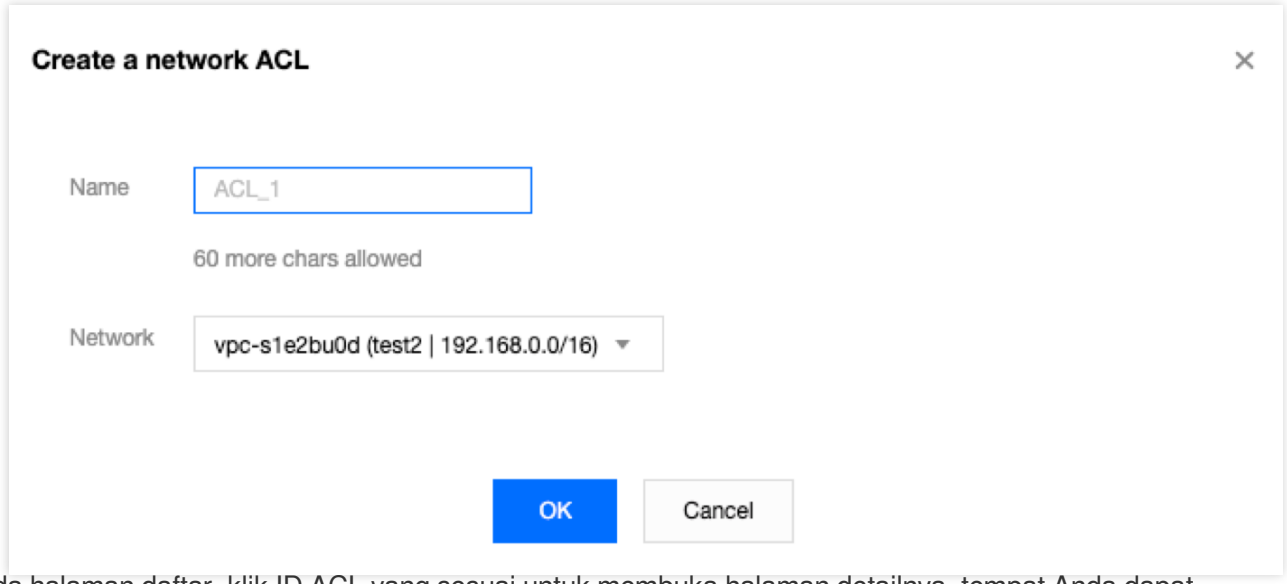
Sumber Daya	Batas
Jumlah ACL jaringan di setiap VPC	50
Jumlah aturan per jaringan ACL	Masuk: 20 Keluar: 20
Jumlah ACL jaringan terhubung ke setiap subnet	1

Mengelola ACL Jaringan

Waktu update terbaru：2024-01-24 17:55:51

Membuat ACL Jaringan

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) -> **Network ACL** (ACL Jaringan) di direktori sebelah kiri untuk membuka halaman manajemen.
3. Pilih wilayah dan VPC di bagian atas daftar dan klik **+New** (+Baru).
4. Masukkan namanya di jendela pop-up, pilih VPC miliknya, dan klik **OK** (Oke).



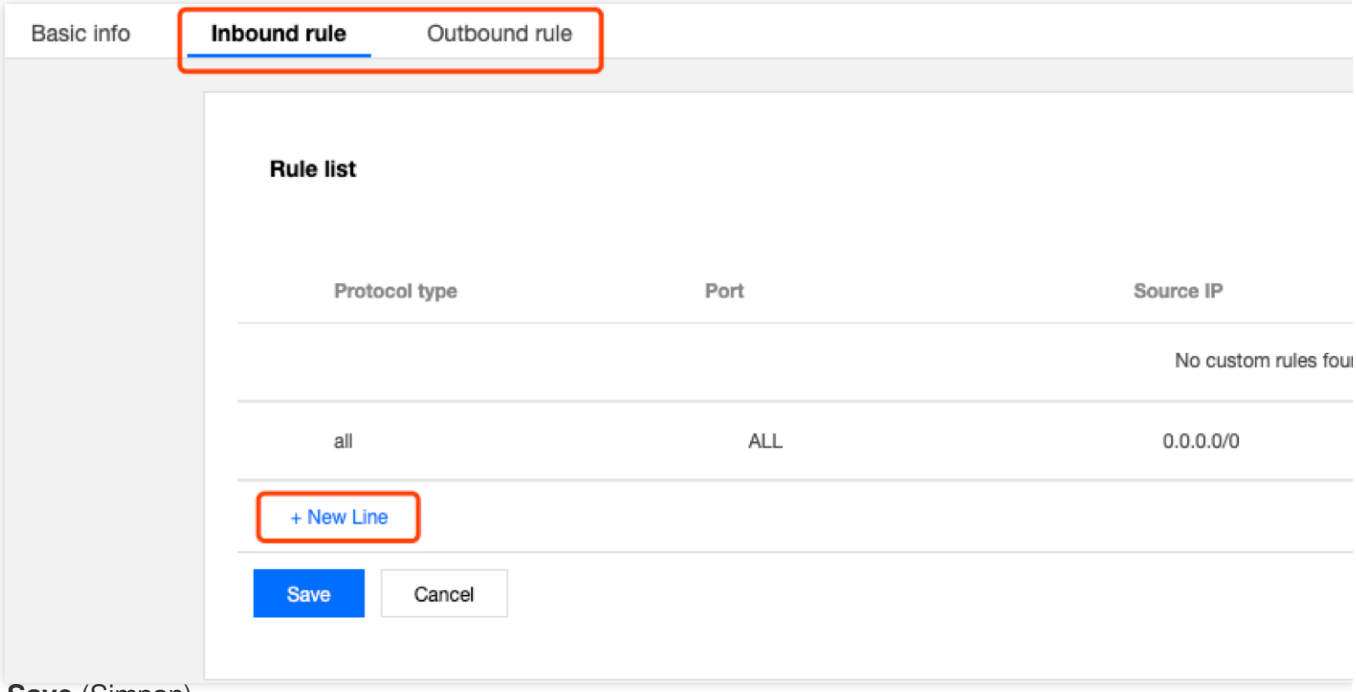
5. Pada halaman daftar, klik ID ACL yang sesuai untuk membuka halaman detailnya, tempat Anda dapat menambahkan aturan ACL dan menghubungkan aturan ACL dengan subnet.

Menambahkan Aturan ACL Jaringan

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) -> **Network ACL** (ACL Jaringan) di direktori sebelah kiri untuk membuka halaman manajemen.
3. Lihat di daftar untuk jaringan ACL yang akan dimodifikasi, dan klik ID-nya untuk membuka halaman detail.
4. Untuk menambahkan aturan keluar/masuk, klik **Outbound Rules** (Aturan Keluar) atau **Inbound Rules** (Aturan Masuk) -> **Edit** -> **New Line** (Baris Baru), pilih jenis protokol, masukkan port dan alamat IP sumber, dan pilih kebijakan.

Jenis protokol: menunjukkan jenis protokol yang diizinkan atau ditolak oleh aturan ACL, misalnya, TCP dan UDP.

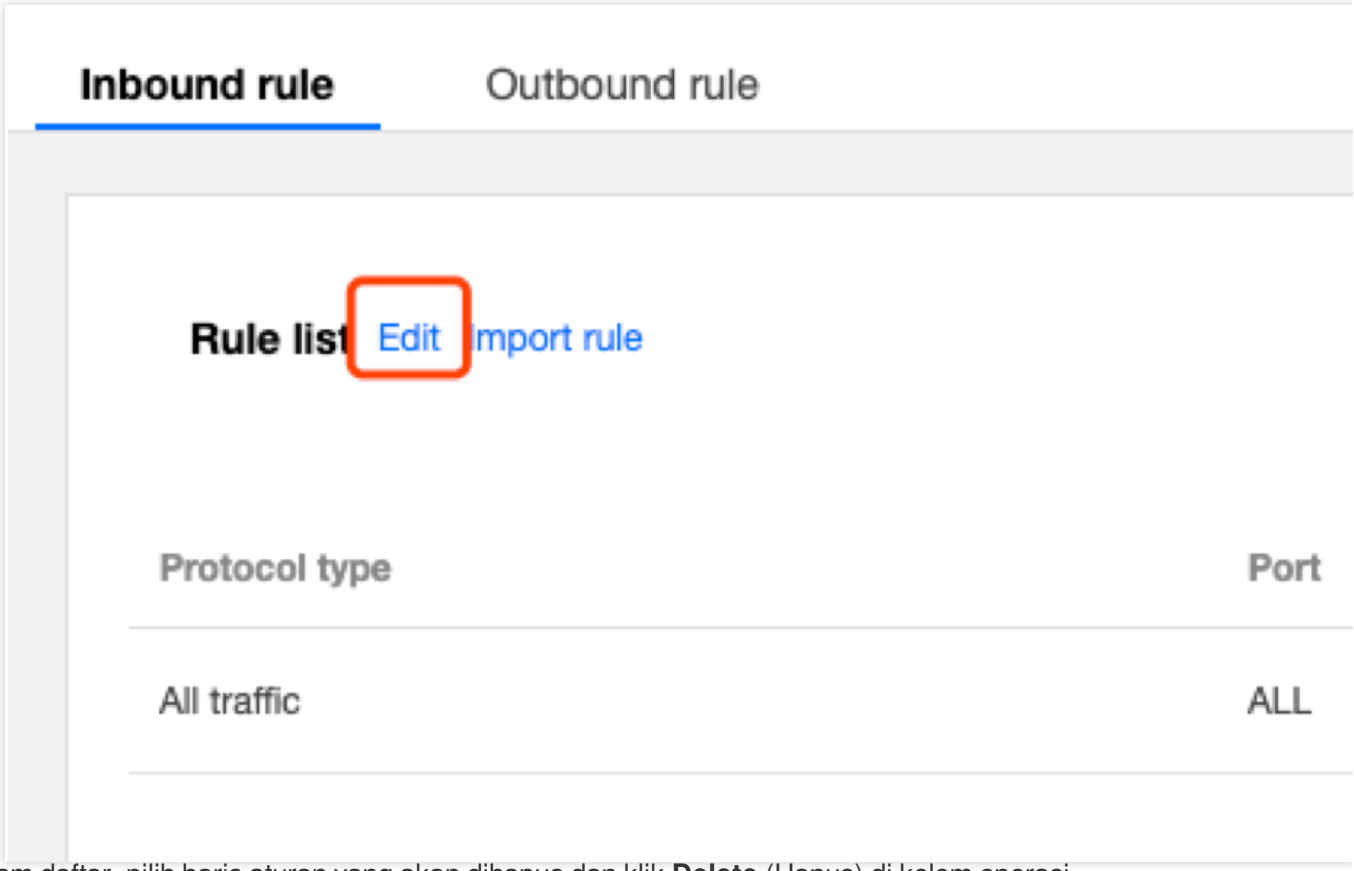
Port: menunjukkan port sumber lalu lintas yang dapat berupa port tunggal atau segmen port, misalnya port 80 atau port 90 hingga 100.
Alamat IP sumber: menunjukkan alamat IP sumber atau rentang IP lalu lintas yang mendukung rentang IP atau blok CIDR, misalnya, `10.20.3.0` atau `10.0.0.2/24` .
Kebijakan: mengizinkan atau menolak permintaan akses.



5. Klik **Save** (Simpan).

Menghapus Aturan ACL Jaringan

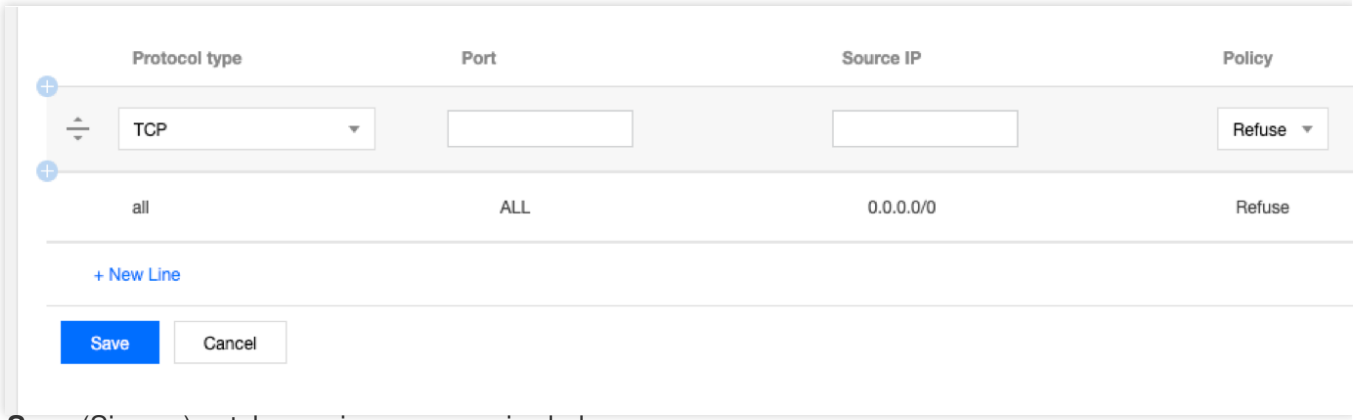
1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) -> **Network ACL** (ACL Jaringan) di direktori sebelah kiri untuk membuka halaman manajemen.
3. Lihat daftar ACL jaringan yang akan dihapus, dan klik ID-nya untuk membuka halaman **Basic Information** (Informasi Dasar).
4. Klik tab **Inbound Rules** (Aturan Masuk) atau tab **Outbound Rules** (Aturan Keluar) untuk membuka halaman **Rules List** (Daftar Aturan).
5. Klik **Edit** (Edit). Proses untuk menghapus aturan masuk sama dengan menghapus aturan keluar. Penghapusan aturan masuk digunakan sebagai contoh di sini.



6. Dalam daftar, pilih baris aturan yang akan dihapus dan klik **Delete** (Hapus) di kolom operasi.

Keterangan:

Aturan ACL ini kini berwarna abu-abu. Jika Anda tidak sengaja menghapusnya, Anda dapat mengeklik **Recover the deleted rule** (Pulihkan aturan yang dihapus) di kolom operasi untuk memulihkan aturan.



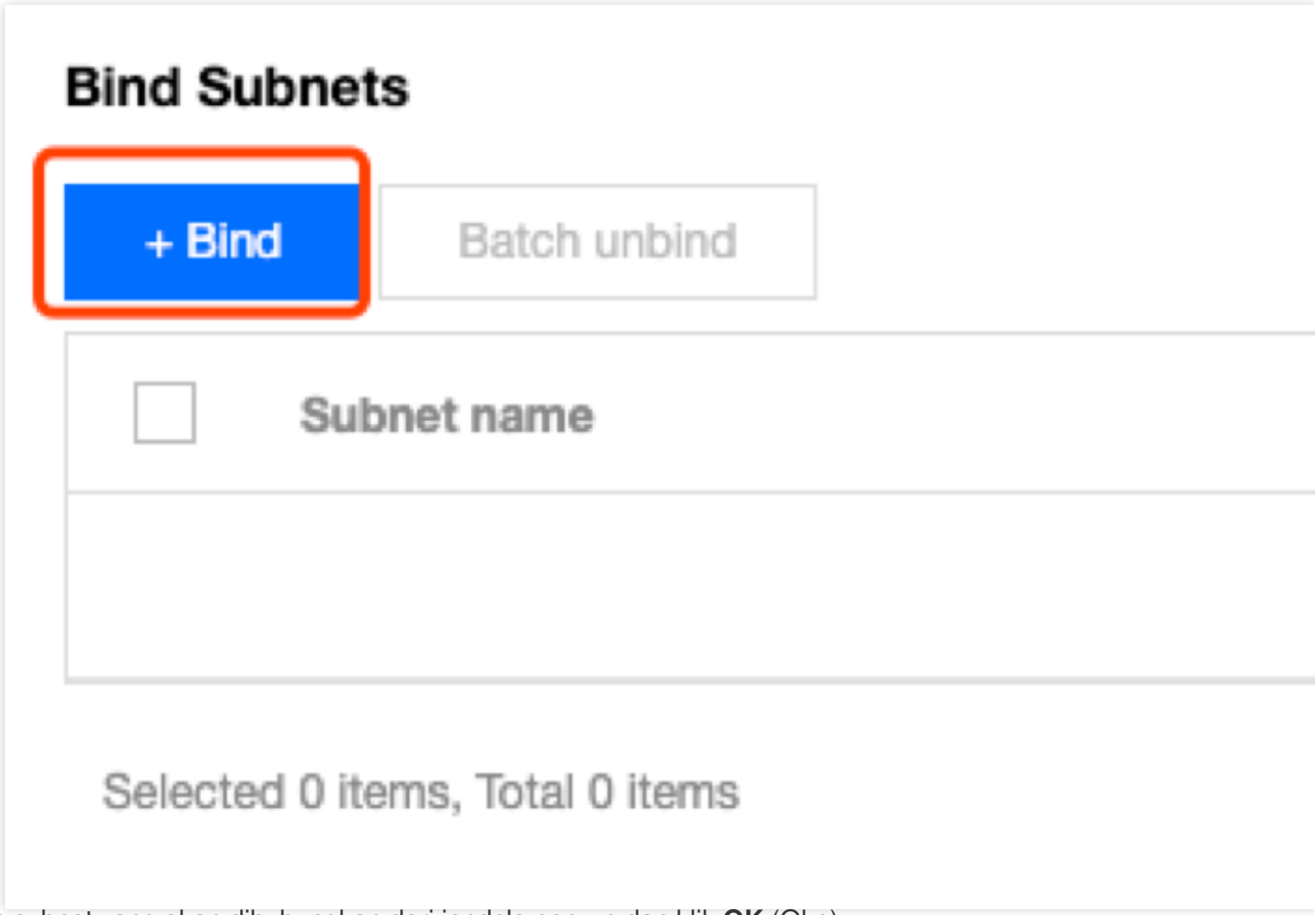
7. Klik **Save** (Simpan) untuk menyimpan operasi sebelumnya.

Perhatian:

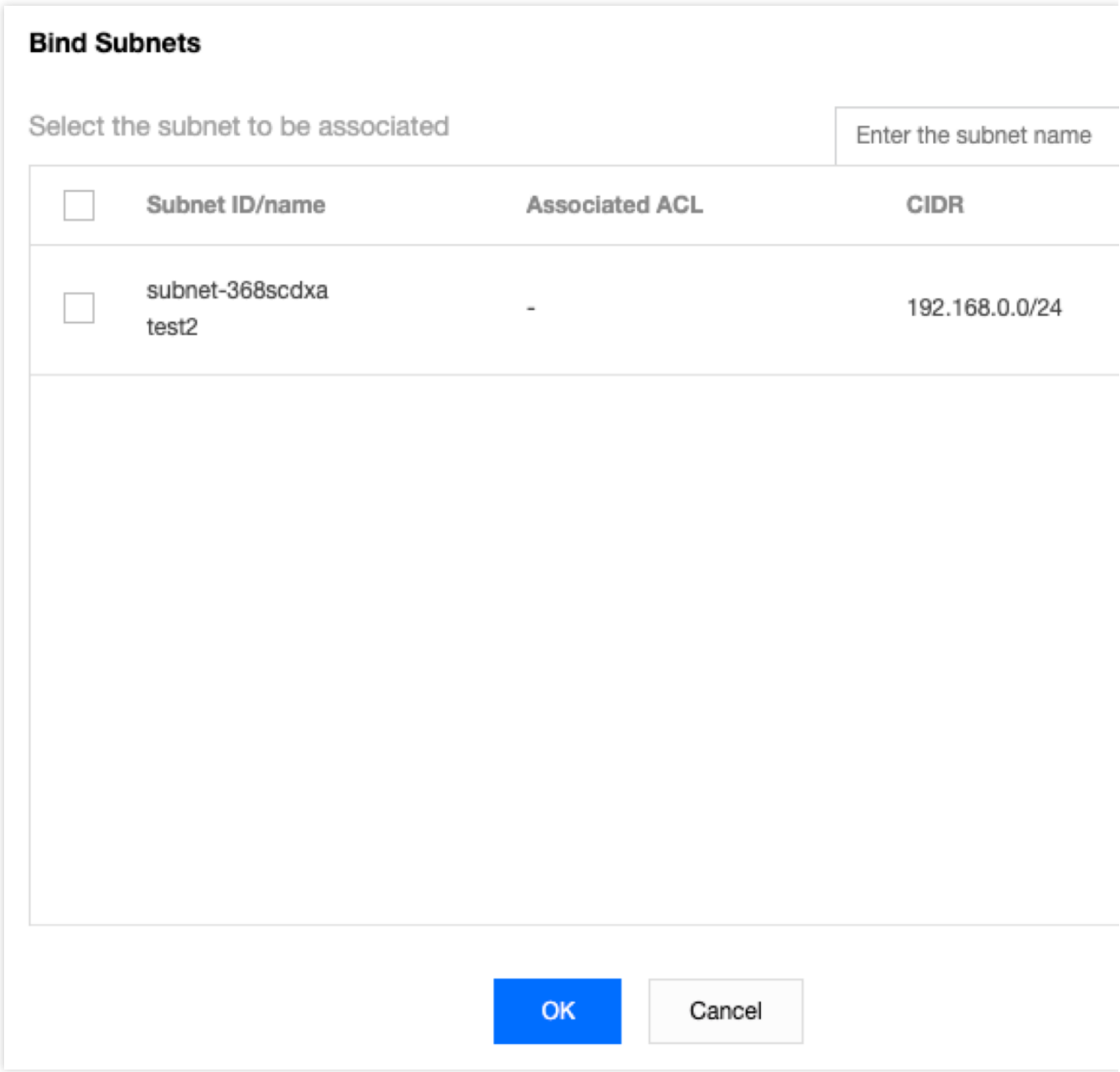
Penghapusan atau pemulihan aturan ACL hanya berlaku setelah Anda menyimpan operasi.

Menghubungkan ACL Jaringan ke Subnet

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) -> **Network ACL** (ACL Jaringan) di direktori sebelah kiri untuk membuka halaman manajemen.
3. Lihat daftar untuk jaringan ACL yang akan dihubungkan, dan klik ID-nya untuk membuka halaman detail.
4. Pada halaman **Basic Information** (Informasi Dasar), klik **Add Association** (Tambahkan Hubungan) di modul **Associated Subnets** (Subnet Terhubung).



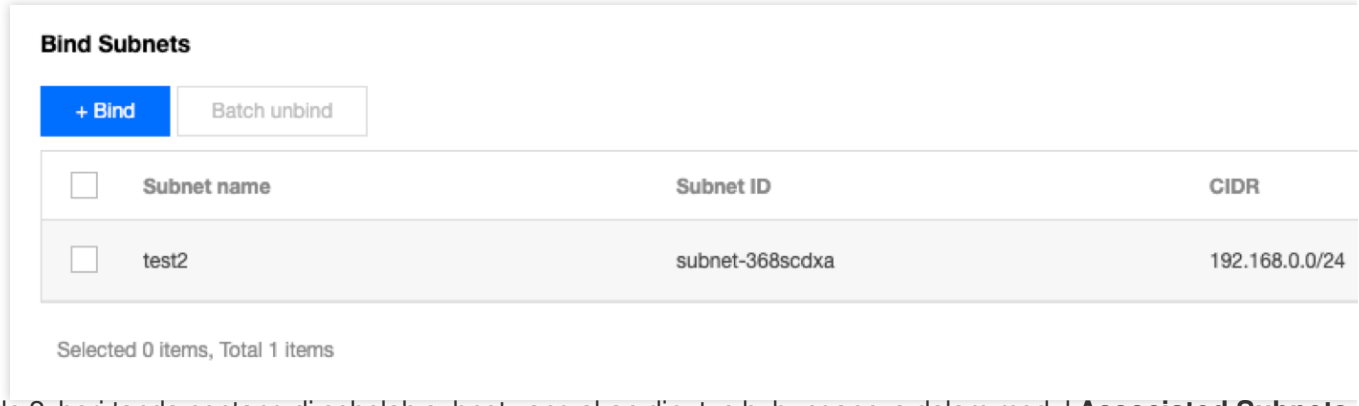
5. Pilih subnet yang akan dihubungkan dari jendela pop-up dan klik **OK** (Oke).



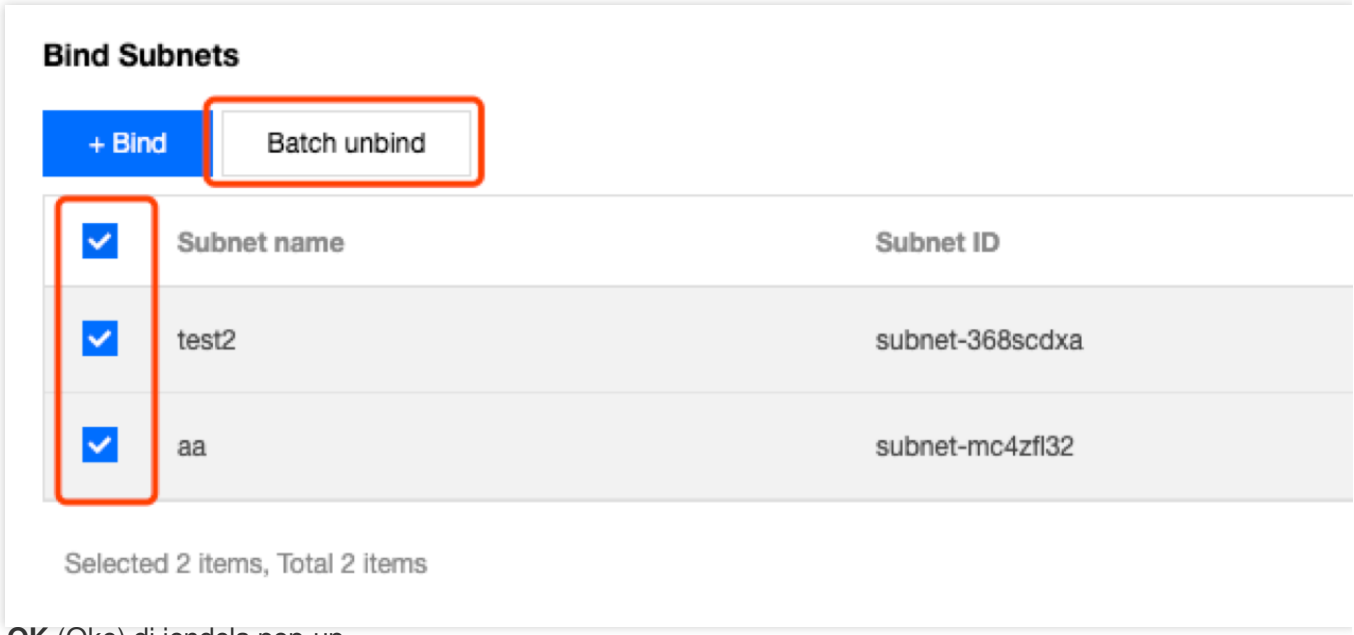
Memutus Hubungan ACL Jaringan dari Subnet

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) -> **Network ACL** (ACL Jaringan) di direktori sebelah kiri untuk membuka halaman manajemen.
3. Lihat daftar untuk jaringan ACL yang akan diputus hubungannya, dan klik ID-nya untuk membuka halaman detail.
4. Ada beberapa metode berbeda untuk memutus hubungan ACL dari subnet:

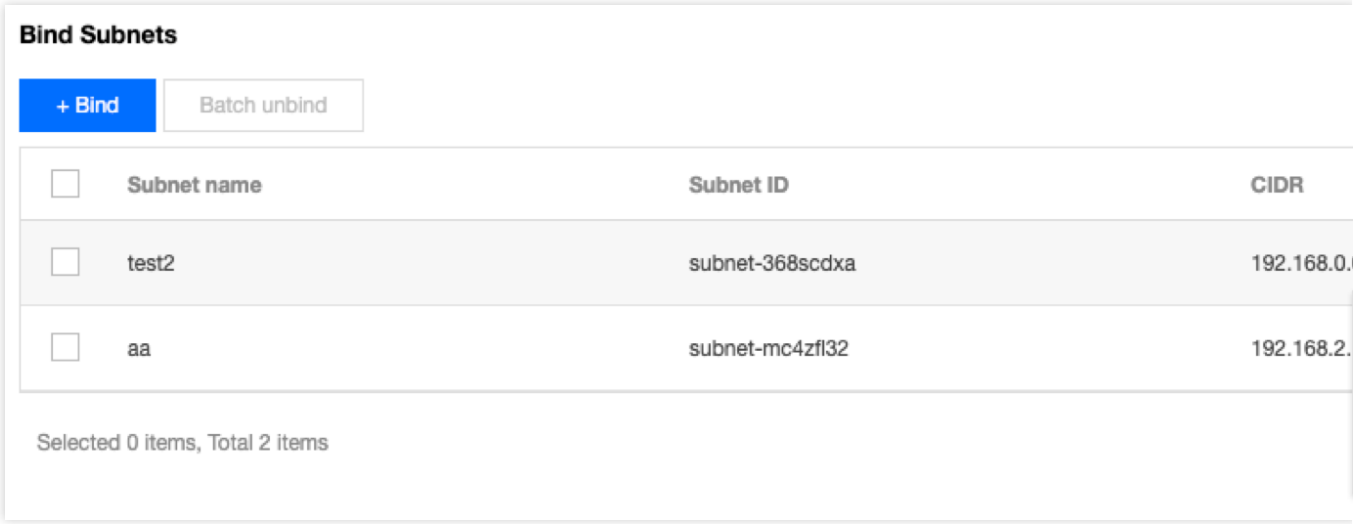
Metode 1: cari subnet yang akan diputus hubungannya di modul **Associated Subnets** (Subnet Terhubung) pada halaman **Basic Information** (Informasi Dasar) dan klik **Disassociate** (Putus Hubungan).



Metode 2: beri tanda centang di sebelah subnet yang akan diputus hubungannya dalam modul **Associated Subnets** (Subnet Terhubung) pada halaman **Basic Information** (Informasi Dasar), dan klik **Batch Disassociate** (Putus Hubungan Batch).



5. Klik **OK** (Oke) di jendela pop-up.

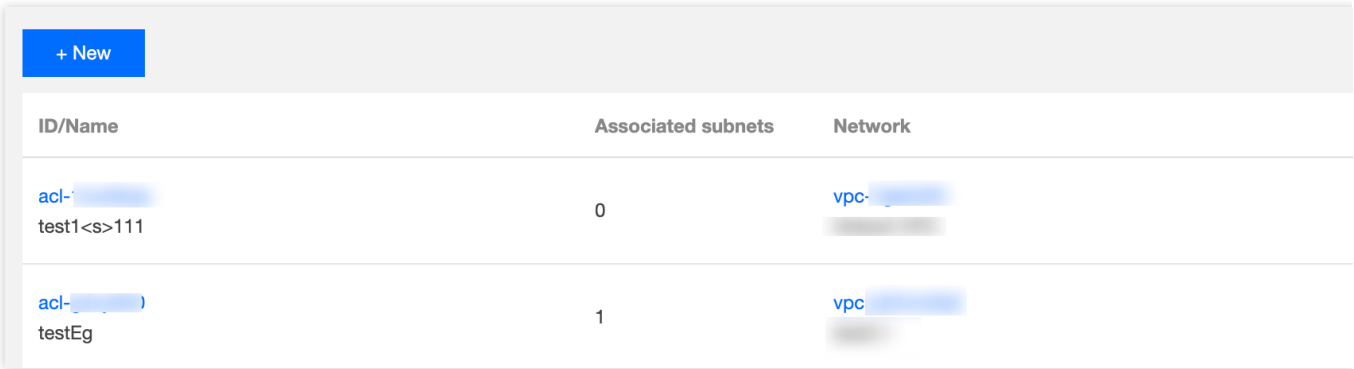


Menghapus ACL Jaringan

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) -> **Network ACL** (ACL Jaringan) di direktori sebelah kiri untuk membuka halaman manajemen.
3. Pilih wilayah dan VPC.
4. Dalam daftar, cari ACL jaringan yang akan dihapus, klik **Delete** (Hapus), lalu konfirmasi penghapusan. ACL jaringan dan semua aturannya akan dihapus.

Keterangan:

Jika opsi **Delete** (Hapus) berwarna abu-abu, seperti untuk jaringan ACL `testEg` pada gambar berikut, ini menunjukkan bahwa ACL jaringan saat ini terhubung ke subnet. Anda harus memutus hubungannya dari subnet terlebih dahulu sebelum dapat menghapusnya.



Templat Parameter

Ikhtisar

Waktu update terbaru：2024-01-24 17:55:51

Templat parameter adalah sekumpulan alamat IP atau parameter port protokol. Anda dapat menyimpan alamat IP dan port protokol sebagai templat agar dapat langsung mengimpor templat saat menambahkan aturan grup keamanan. Templat parameter, jika digunakan dengan benar, dapat meningkatkan efisiensi Anda dalam menggunakan grup keamanan.

Kasus Penggunaan

Templat parameter terutama cocok untuk skenario berikut:
Mengelola beberapa alamat IP atau grup port protokol dengan persyaratan yang sama.
Mengelola beberapa alamat IP atau grup port protokol dengan kebutuhan pengeditan berulang.

Jenis Templat Parameter

Tencent Cloud mendukung empat jenis templat parameter:
Alamat IP: juga dikenal sebagai objek alamat IP, templat ini adalah kumpulan alamat IP dan mendukung satu IP tunggal, blok CIDR, dan rentang IP.
Grup alamat IP: juga dikenal sebagai objek grup alamat IP, templat ini adalah sekumpulan beberapa objek alamat IP.
Port protokol: juga dikenal sebagai objek port protokol, templat ini adalah sekumpulan port protokol dan mendukung satu port tunggal, beberapa port, rentang port, dan semua port. Protokol yang didukung adalah TCP, UDP, ICMP, dan GRE.
Grup port protokol: juga dikenal sebagai objek grup port protokol, templat ini adalah sekumpulan objek port protokol.

Batasan

Waktu update terbaru：2024-01-24 17:55:51

Batasan Penggunaan

Format yang didukung oleh templat alamat IP adalah sebagai berikut:

Alamat IP tunggal: seperti `10.0.0.1` ;

Alamat IP beruntun: seperti `10.0.0.1` - `10.0.0.100` ;

Rentang IP: seperti `10.0.1.0/24` .

Format yang didukung oleh templat port adalah sebagai berikut:

Port tunggal: seperti `TCP:80` ;

Beberapa port: seperti `TCP:80,443` ;

Rentang port: seperti `TCP:3306-20000` ;

Semua port: seperti `TCP:ALL` .

Batasan Kuota

Instans	Batas Atas
Objek alamat IP (ipm)	1.000 per penyewa
Objek grup alamat IP (ipmg)	1.000 per penyewa
Objek port protokol (ppm)	1.000 per penyewa
Objek grup port protokol (ppmg)	1.000 per penyewa
Anggota alamat IP dalam objek alamat IP (ipm)	20 per penyewa
Anggota objek alamat IP (ipm) dalam objek grup alamat IP (ipmg)	20 per penyewa
Anggota port protokol dalam objek grup port protokol (ppm)	20 per penyewa
Anggota objek port protokol (ppm) dalam objek grup port protokol (ppmg)	20 per penyewa
Objek grup alamat IP (ipmg) yang dapat mereferensikan objek alamat IP yang sama (ipm)	50 per penyewa
Objek grup port protokol (ppmg) yang dapat mereferensikan objek port protokol yang sama (ppm)	50 per penyewa

Keterangan:

Jika templat parameter direferensikan oleh grup keamanan, IP dan port dalam templat akan dikonversi ke beberapa aturan grup keamanan (hingga 2000).

Manajemen Templat Parameter

Waktu update terbaru：2024-01-24 17:55:51

Dokumen ini menjelaskan cara membuat dan memelihara templat parameter (alamat IP, grup alamat IP, port protokol, dan grup port protokol) di konsol dan cara menggunakannya di grup keamanan.

Membuat Templat Parameter

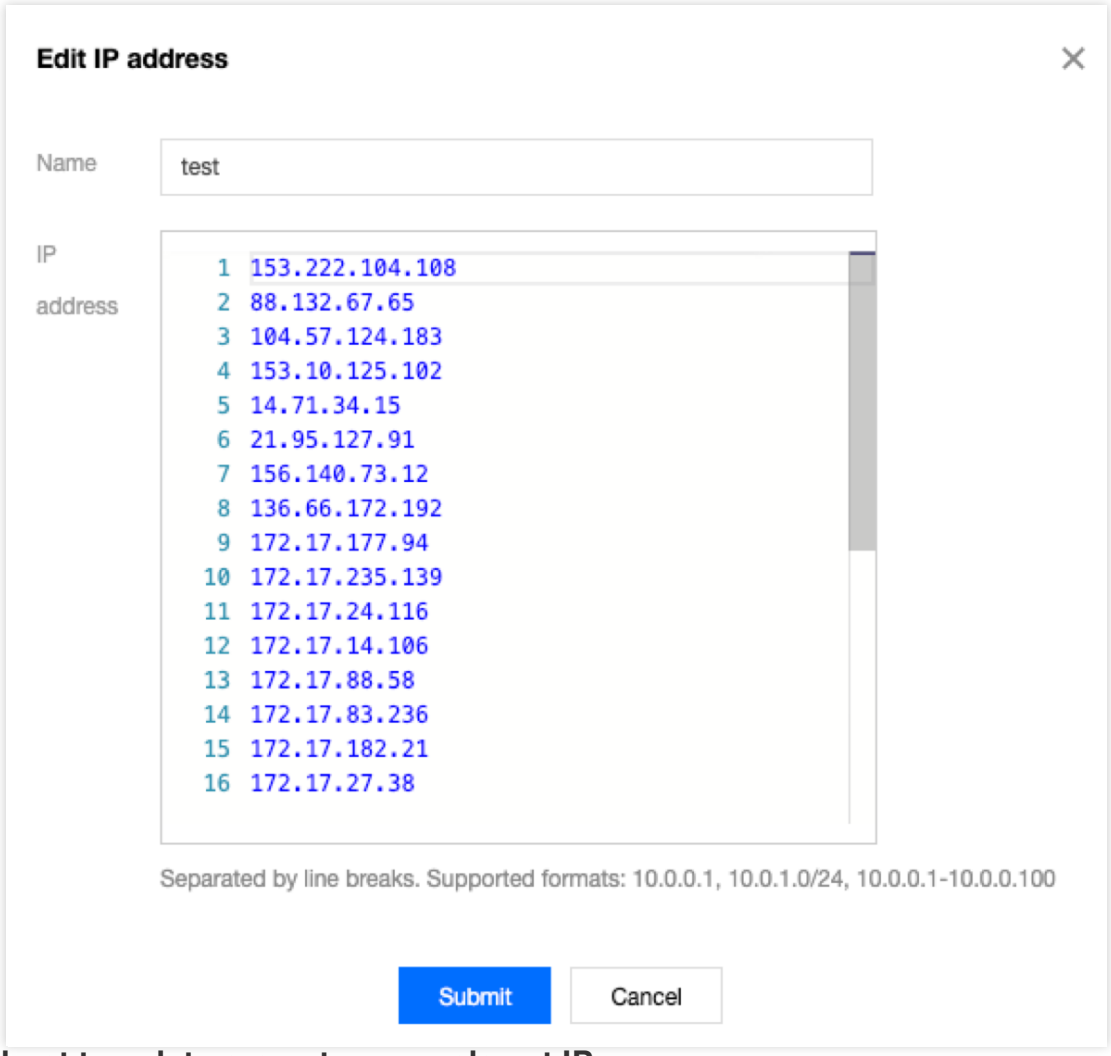
Membuat templat parameter alamat IP

Tambahkan IP dengan kebutuhan yang sama atau yang sering diedit ke objek alamat IP ini.

Petunjuk

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) > **Parameter Template** (Templat Parameter) di bilah sisi kiri untuk membuka halaman pengelolaan.
3. Pilih tab **IP Address** (Alamat IP) dan klik **+ New** (+ Baru).
4. Pada jendela pop-up, masukkan nama dan alamat IP, lalu klik **Submit** (Kirim).

Anda dapat menambahkan beberapa alamat IPv4 dalam rentang berikut dan memisahkannya menurut jeda baris:
Alamat IP tunggal: seperti `10.0.0.1` ;
Blok CIDR: seperti `10.0.1.0/24` ;
Rentang IP: seperti `10.0.0.1` - `10.0.0.100` .

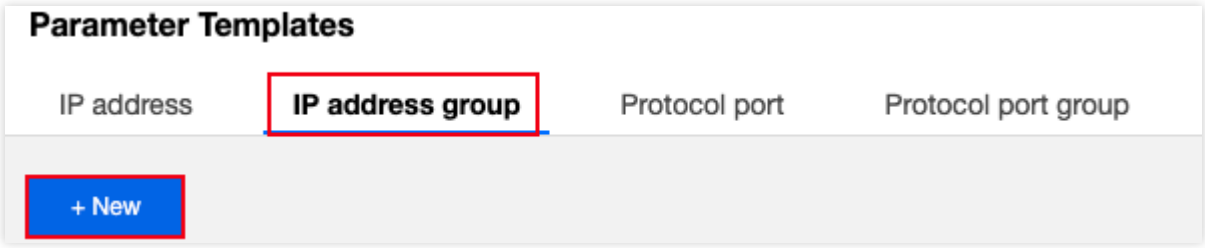


Membuat templat parameter grup alamat IP

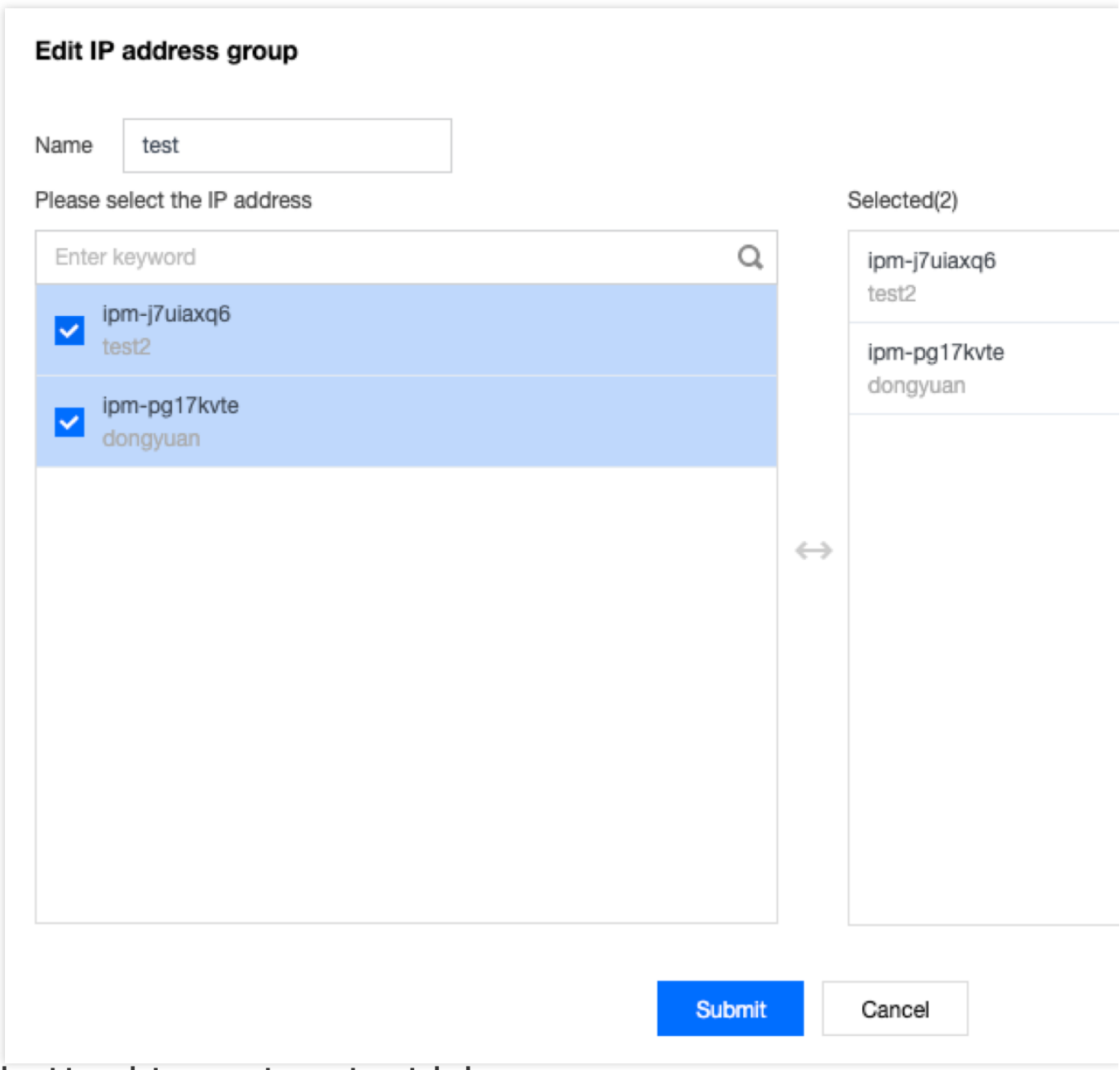
Anda dapat menambahkan beberapa objek alamat IP ke grup alamat IP untuk pengelolaan terpadu.

Petunjuk

1. Pilih tab **IP Address Group** (Grup Alamat IP) dan klik **+ New** (+ Baru).



2. Pada jendela pop-up, masukkan nama, pilih objek alamat IP yang ingin Anda tambahkan, lalu klik **Submit** (Kirim).



Membuat templat parameter port protokol

Tambahkan port protokol dengan kebutuhan yang sama atau yang sering diedit ke objek port protokol ini.

Petunjuk

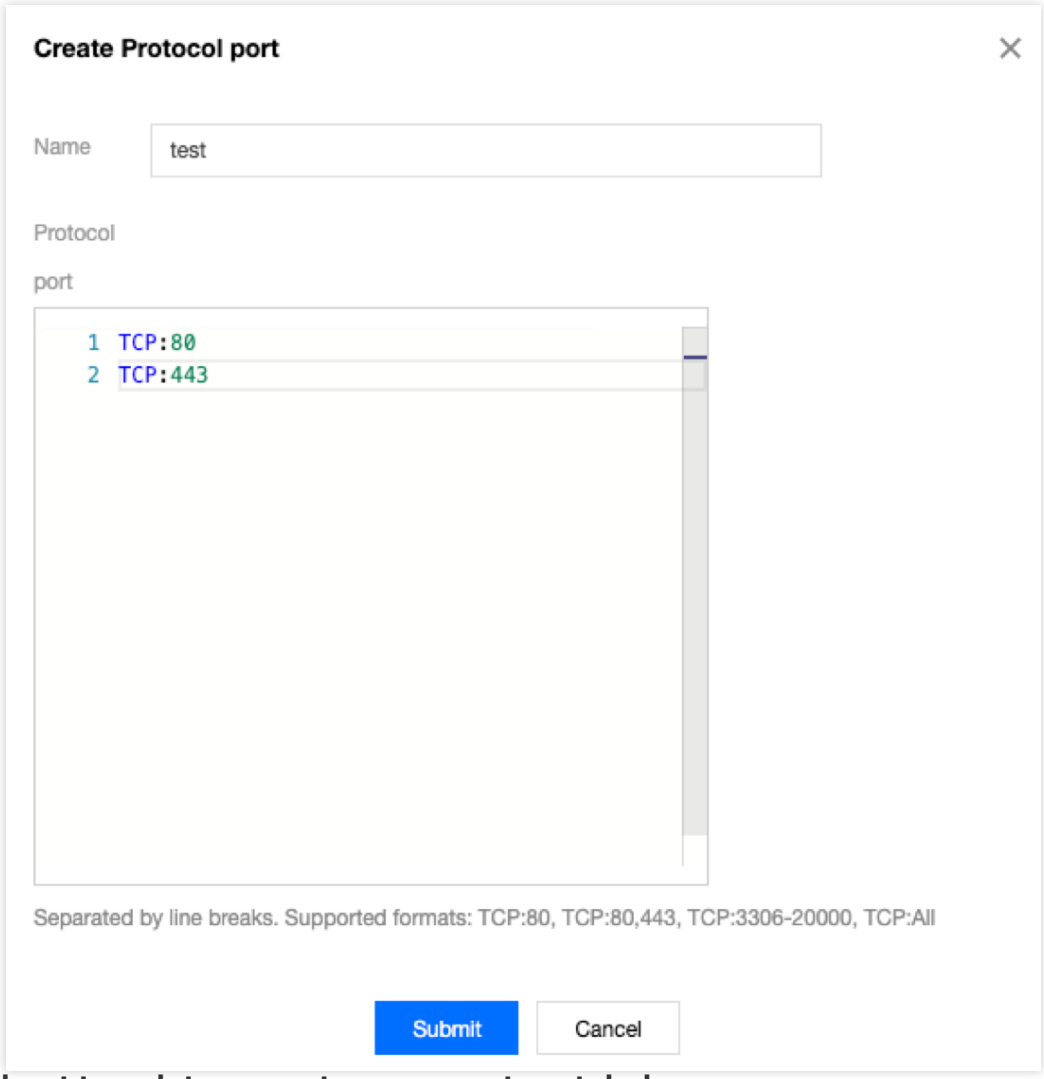
1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) > **Parameter Template** (Templat Parameter) di bilah sisi kiri untuk membuka halaman pengelolaan.
3. Pilih tab **Protocol Port** (Port Protokol) dan klik **+ New** (+ Baru).
4. Pada jendela pop-up, masukkan nama dan port protokol, dan klik **Submit** (Kirim).

Anda dapat menambahkan beberapa port protokol dalam rentang berikut dan memisahkannya dengan jeda baris:

Port tunggal: seperti `TCP:80` ;

Beberapa port: seperti `TCP:80,443` ;

Rentang port: seperti `TCP:3306-20000` ;
Semua port: seperti `TCP:ALL` .

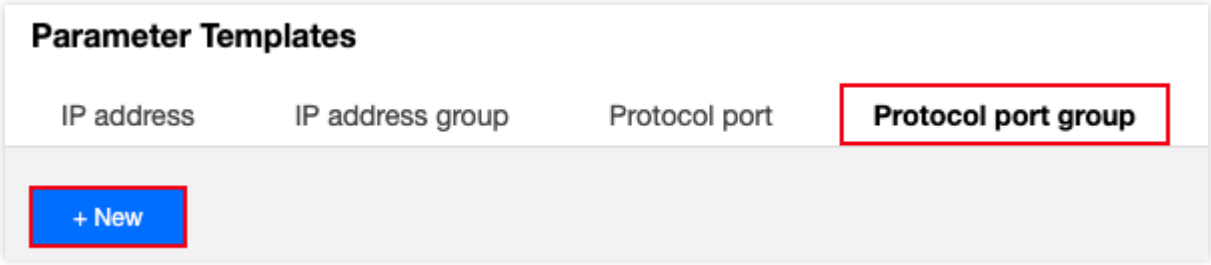


Membuat templat parameter grup port protokol

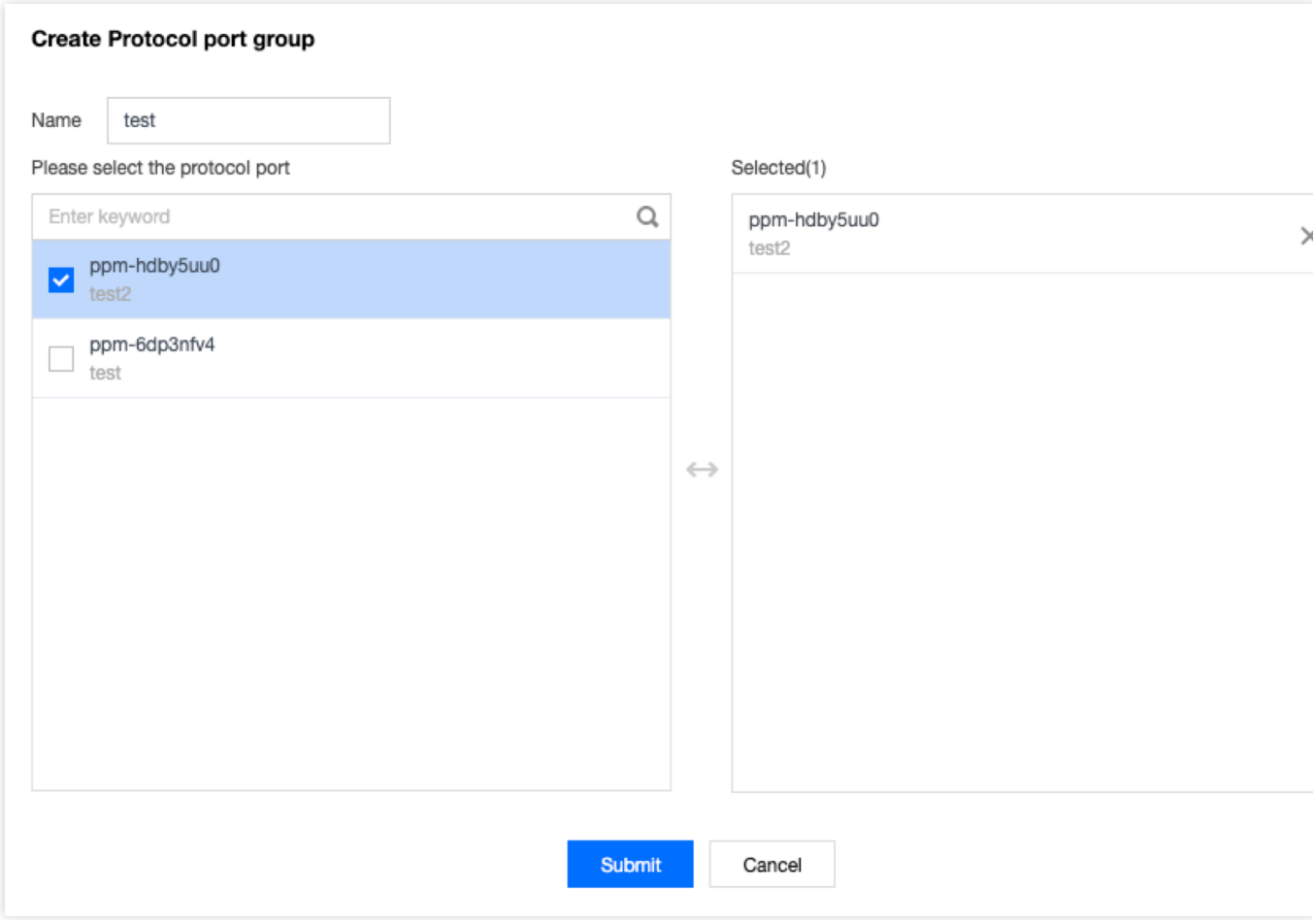
Anda dapat menambahkan beberapa objek port protokol yang dibuat ke grup port protokol untuk pengelolaan terpadu.

Petunjuk

1. Pilih tab **Protocol Port Group** (Grup Port Protokol) dan klik **+ New** (+ Baru).



2. Pada jendela pop-up, masukkan nama, pilih objek port protokol yang akan ditambahkan, lalu klik **Submit** (Kirim).

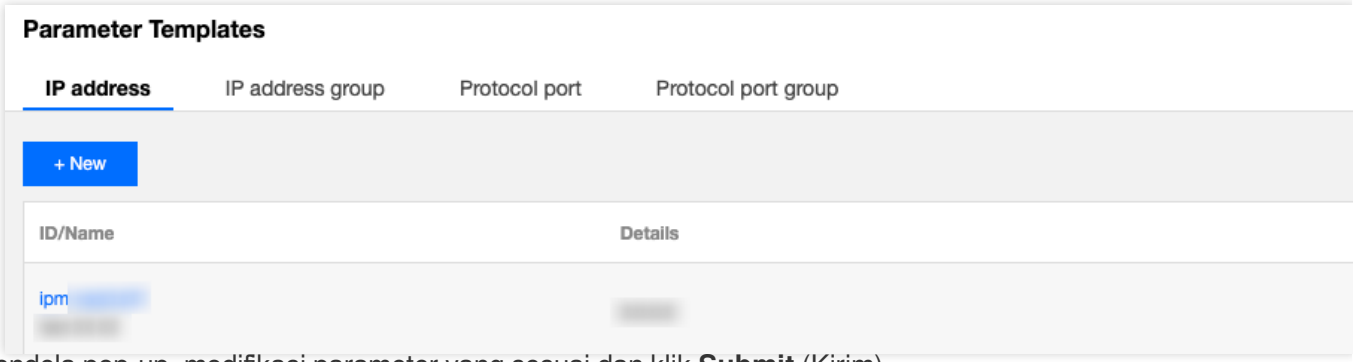


Memodifikasi Templat Parameter

Jika Anda perlu memodifikasi templat parameter yang dibuat, misalnya, untuk menambah/menghapus alamat IP atau port protokol, ikuti langkah-langkah di bawah ini.

Petunjuk

1. Klik alamat IP, grup alamat IP, port protokol, atau templat parameter grup port protokol yang dibuat dan klik **Edit** (Edit) di sebelah kanan. Misalnya, gambar berikut menunjukkan cara memodifikasi objek alamat IP.



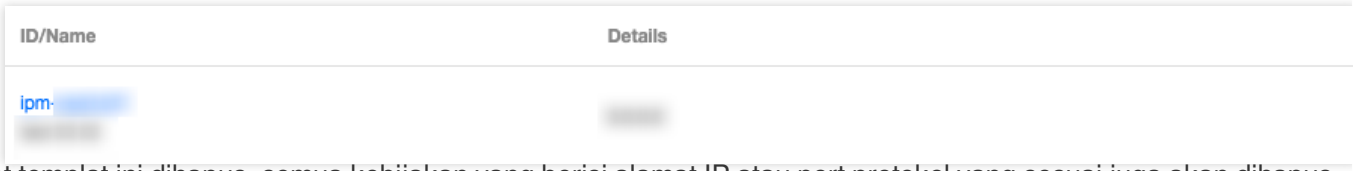
2. Di jendela pop-up, modifikasi parameter yang sesuai dan klik **Submit** (Kirim).

Menghapus Templat Parameter

Jika Anda tidak lagi menggunakan templat parameter, Anda dapat menghapusnya. Saat templat ini dihapus, semua konfigurasi kebijakan yang memuatnya dalam grup keamanan akan dihapus secara bersamaan. Harap evaluasi dan lanjutkan dengan hati-hati.

Petunjuk

1. Klik **Delete** (Hapus) di sebelah kanan templat parameter yang dibuat.



2. Saat templat ini dihapus, semua kebijakan yang berisi alamat IP atau port protokol yang sesuai juga akan dihapus. Setelah mengonfirmasi bahwa semua langkah sudah benar, klik **Delete** (Hapus) di jendela pop-up **Confirm Deletion** (Konfirmasi Penghapusan).

Mengimpor Templat Parameter ke dalam Grup Keamanan

Setelah membuat templat parameter, Anda dapat langsung mengimpornya saat menambahkan aturan dalam grup keamanan untuk menambahkan sumber IP atau port protokol dengan cepat, yang membantu meningkatkan efisiensi Anda dalam menambahkan aturan grup keamanan.

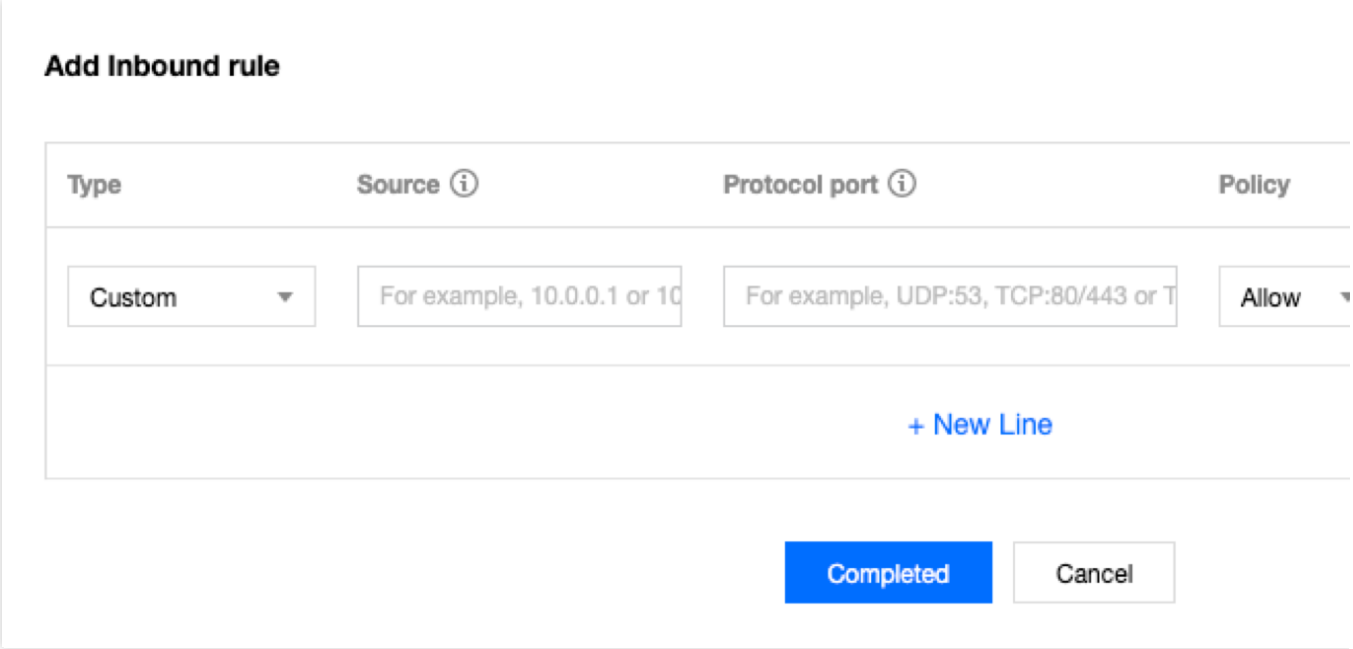
Petunjuk

1. Login ke Konsol VPC.
2. Klik **Security** (Keamanan) > **Security Group** (Grup Keamanan) di bilah sisi kiri untuk membuka halaman pengelolaan.

3. Dalam daftar, temukan grup keamanan tempat templat parameter perlu diimpor, dan klik ID-nya untuk masuk ke halaman detail.
4. Pada tab **Inbound/Outbound Rules** (Aturan Masuk/Keluar), klik **Add Rule** (Tambahkan Aturan).
5. Di jendela pop-up, pilih jenis **Custom** (Kustom), pilih templat parameter yang dibuat di **Source** (Sumber) dan **Protocol Port** (Port Protokol), lalu klik **Complete** (Selesai). Untuk informasi selengkapnya tentang cara menambahkan aturan masuk/keluar, harap lihat Menambahkan Aturan Grup Keamanan.

Keterangan:

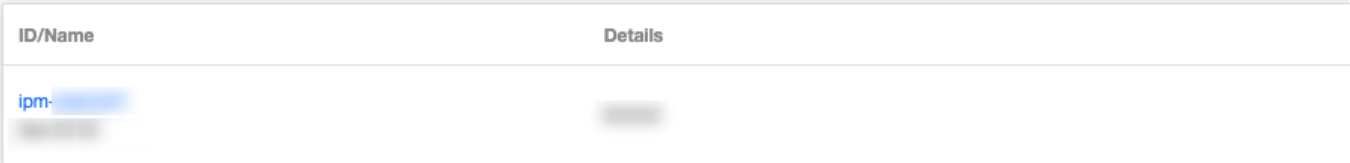
Jika Anda perlu menambahkan alamat IP atau port protokol baru di masa mendatang, Anda hanya perlu menambahkannya ke grup alamat IP atau grup port protokol yang sesuai, dan tidak perlu memodifikasi aturan grup keamanan atau membuat grup keamanan lain.



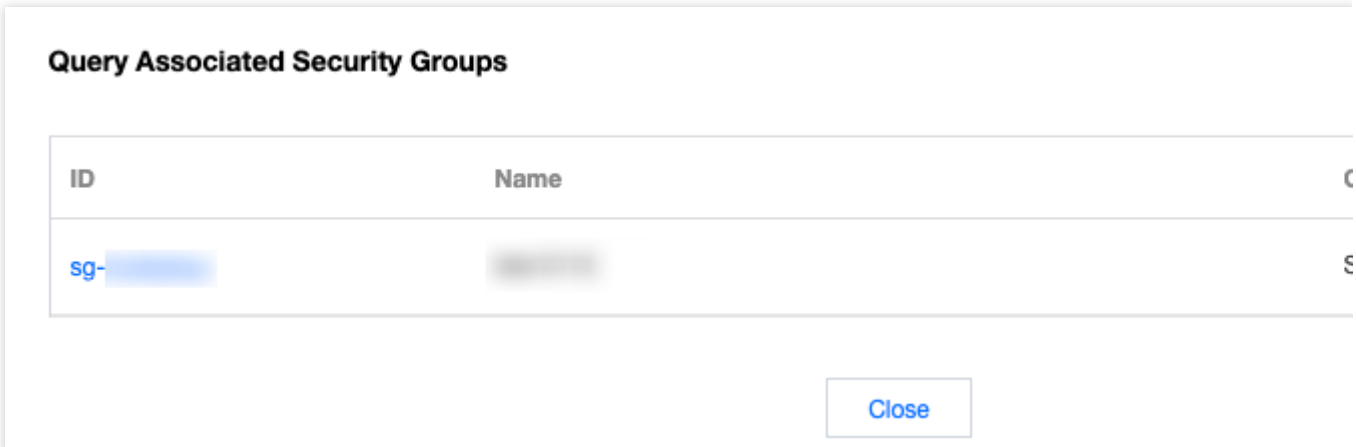
Melihat Grup Keamanan yang Dihubungkan

Anda dapat melihat semua instans grup keamanan yang mengimpor templat parameter dalam langkah-langkah berikut.

1. Klik **View Association** (Lihat Hubungan) di sebelah kanan templat parameter yang dibuat.



2. Daftar grup keamanan terhubung yang muncul menampilkan semua instans grup keamanan yang terhubung dengan templat parameter ini.



Kasus Konfigurasi

Waktu update terbaru：2024-01-24 17:55:51

Kasus Penggunaan Templat Parameter

Templat parameter adalah cara yang efisien, cepat, dan mudah dipelihara untuk menambahkan aturan dalam grup keamanan. Misalnya, saat Anda perlu menambahkan beberapa rentang IP, IP yang telah ditentukan, atau port protokol dari beberapa jenis, Anda dapat menentukan templat parameter. Anda juga dapat menggunakan templat parameter selanjutnya untuk mempertahankan sumber IP dan port protokol dalam aturan grup keamanan.

Keterangan:

Semua alamat IP dan port protokol dalam dokumen ini adalah contoh. Harap ganti sesuai kondisi bisnis aktual Anda selama konfigurasi.

Deskripsi Contoh

Misalnya Anda ingin mengonfigurasi aturan grup keamanan berikut dan nantinya perlu memperbarui rentang IP sumber masuk dan port protokol:

Aturan masuk:

Rentang IP sumber yang diizinkan: 10.0.0.16-10.0.0.30; port protokol: TCP:80,443

Blok CIDR sumber yang diizinkan: 192.168.3.0/24; port protokol: TCP:3600-15000

Aturan keluar:

Alamat IP target yang ditolak: 192.168.10.4; port protokol: TCP:800

Solusi

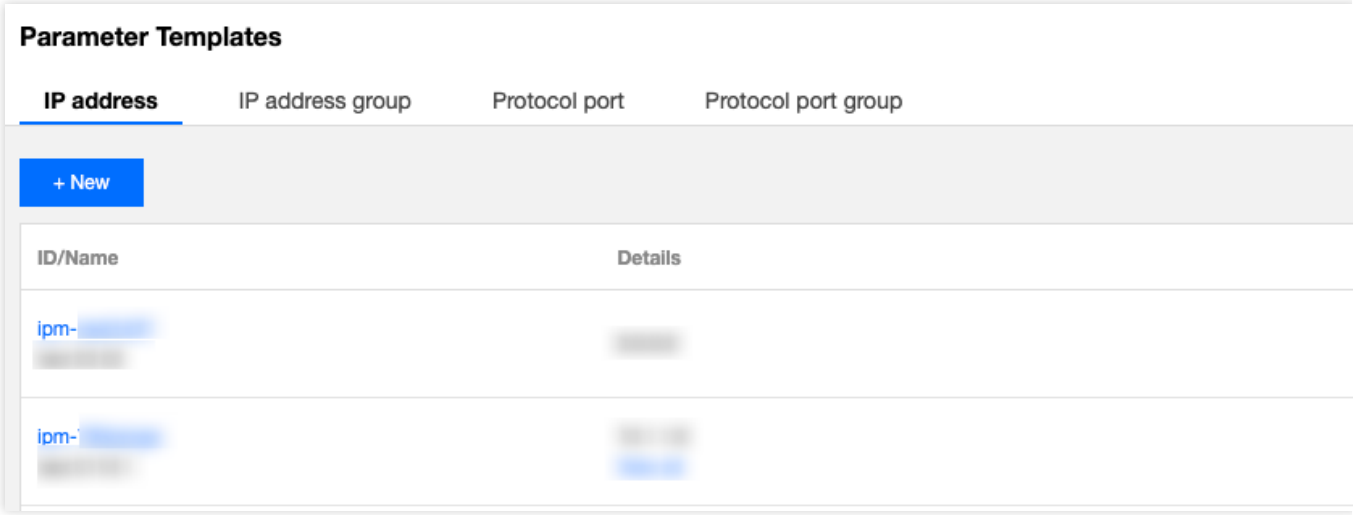
Karena Anda memiliki kebijakan grup keamanan yang sama untuk beberapa rentang IP dan port protokol, dan Anda nantinya perlu memperbarui rentang IP sumber, Anda dapat menggunakan templat parameter untuk menerapkan penambahan dan pemeliharaan aturan grup keamanan.

Langkah 1. Buat templat parameter

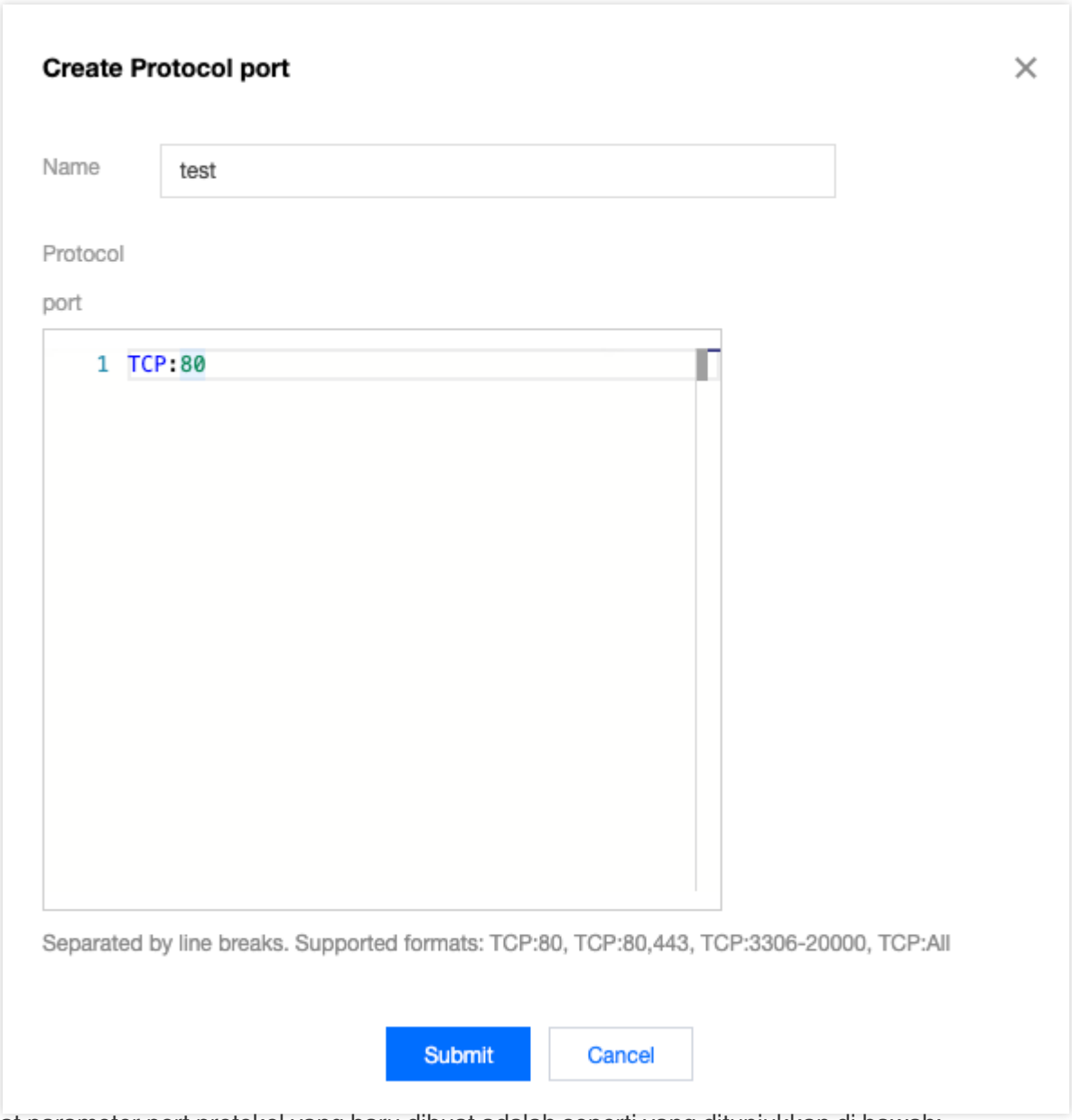
1. Login ke Konsol VPC.
2. Pilih **Security** (Keamanan) > **Parameter Template** (Templat Parameter) di bilah sisi kiri untuk mengakses halaman manajemen.
3. Pada tab **IP Address** (Alamat IP), klik **+ New** (+Baru) guna membuat templat parameter alamat IP untuk menambahkan aturan masuk dan keluar.

4. Di jendela pop-up, masukkan rentang IP sumber dan klik **Submit** (Kirim).

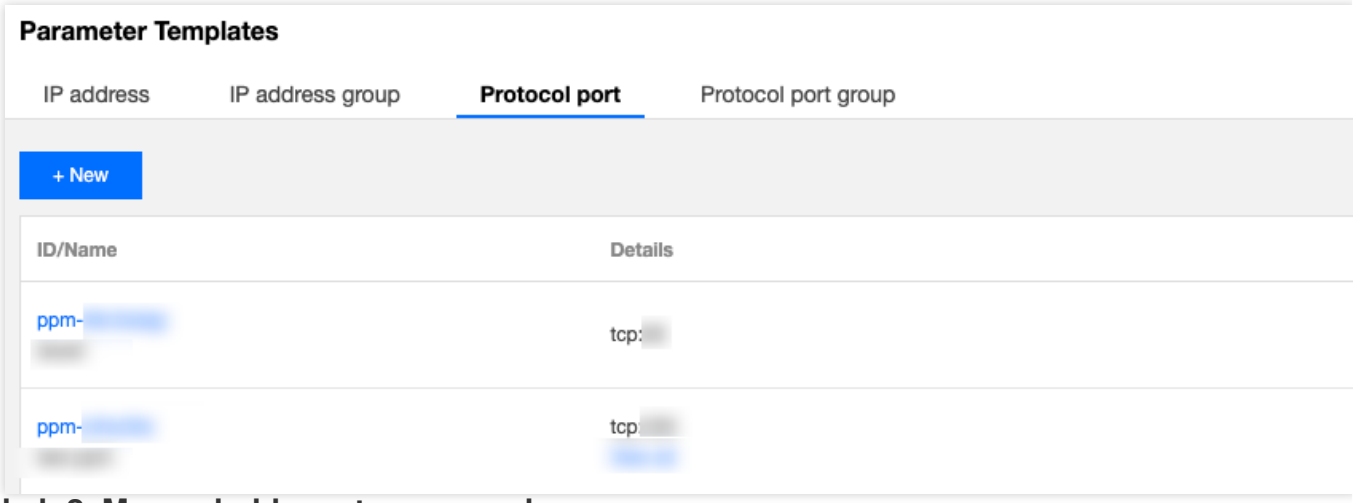
Templat parameter alamat IP yang baru dibuat adalah seperti yang ditunjukkan di bawah.



5. Pada tab **Protocol Port** (Port Protokol), klik **+ New** (+Baru) untuk membuat templat parameter port protokol guna menambahkan aturan masuk dan keluar.

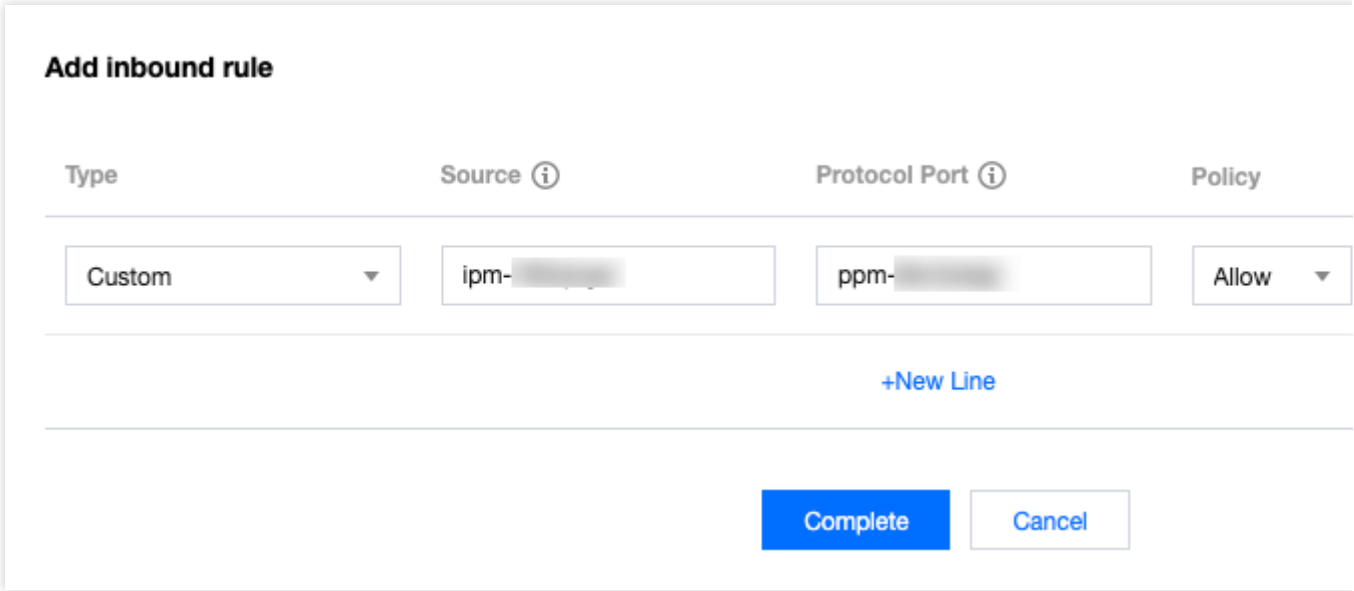


Templat parameter port protokol yang baru dibuat adalah seperti yang ditunjukkan di bawah:



Langkah 2. Menambahkan aturan grup keamanan

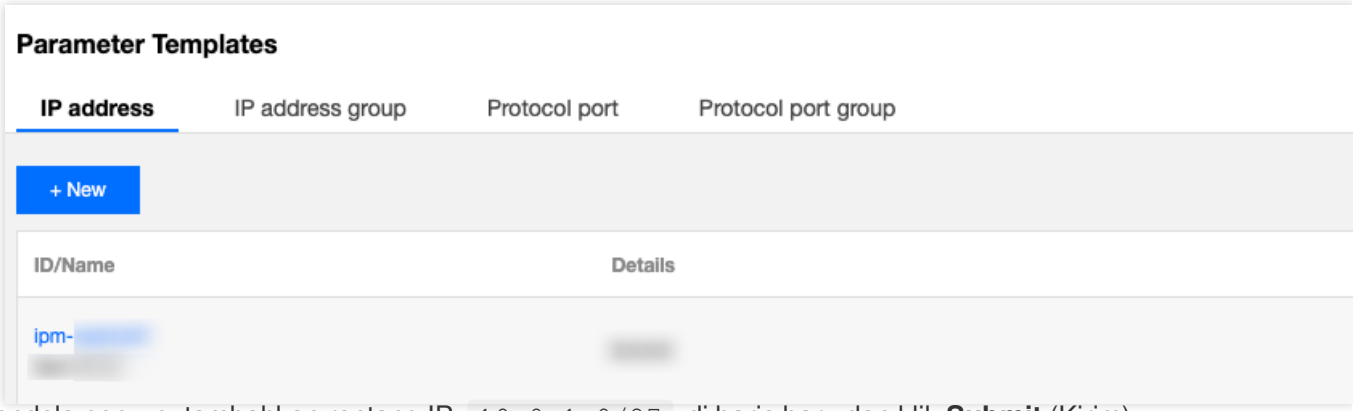
1. Login ke Konsol VPC.
2. Pilih **Security** (Keamanan) > **Security Group** (Grup Keamanan) di bilah sisi kiri untuk mengakses halaman manajemen.
3. Dalam daftar, temukan grup keamanan yang perlu mengimpor templat parameter dan klik ID-nya untuk masuk ke halaman detail.
4. Pada halaman tab **Inbound Rules or Outbound Rules** (Aturan Masuk atau Aturan Keluar), klik **Add Rules** (Tambahkan Aturan).
5. Di jendela pop-up, pilih jenis kustom, pilih templat parameter alamat IP yang sesuai untuk sumber/target, pilih templat parameter port protokol yang sesuai untuk port protokol tersebut, dan klik **Complete** (Selesai).



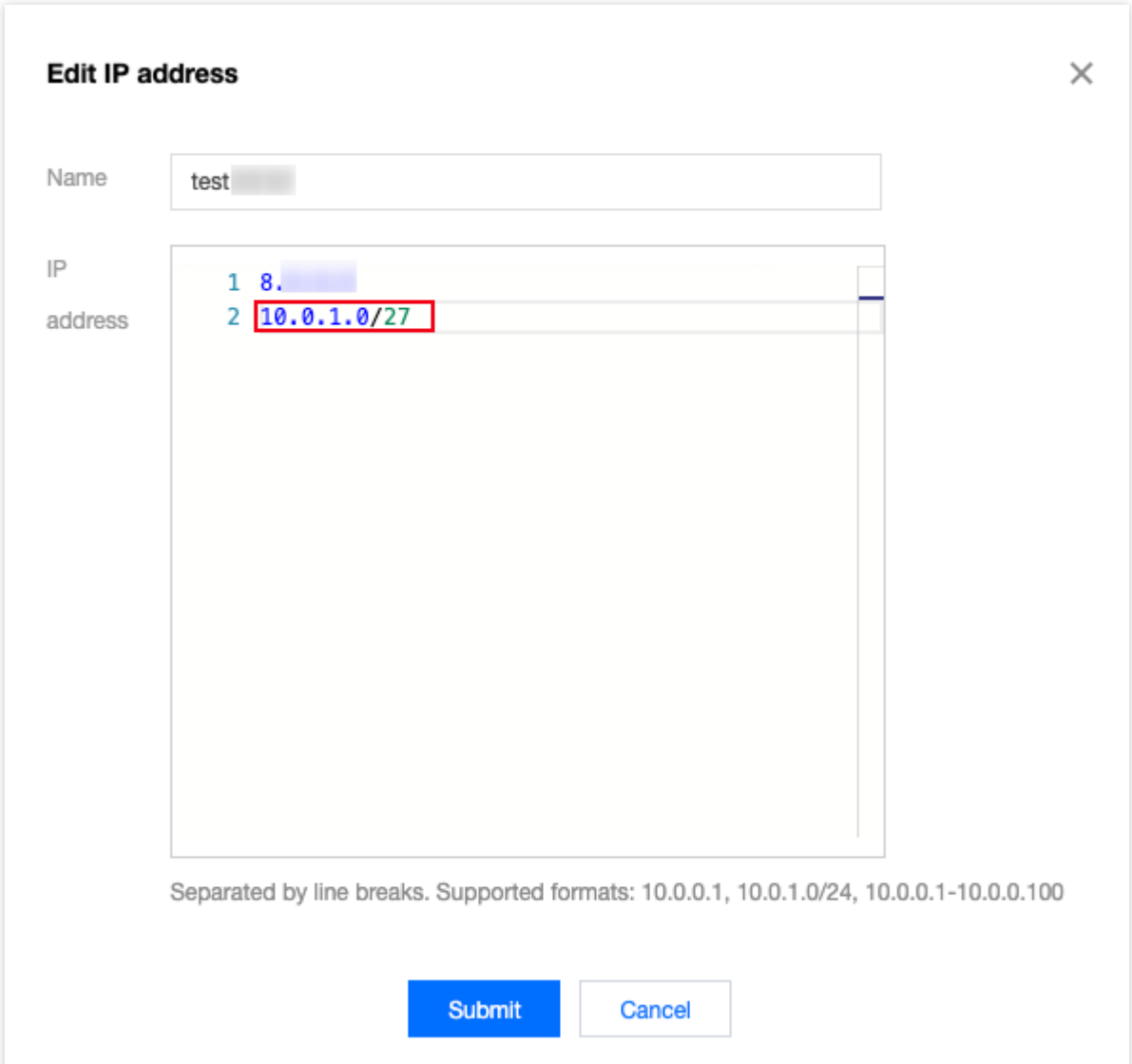
Langkah 3. Memperbarui templat parameter

Misalkan Anda perlu menambahkan aturan masuk dengan sumber IP sebagai rentang IP `10.0.1.0/27` dan port protokol menjadi `UDP:58` . Anda dapat langsung memperbarui templat parameter alamat IP `ipm-0ge3ob8e` dan port protokol `ppm-4ty1ck3i` .

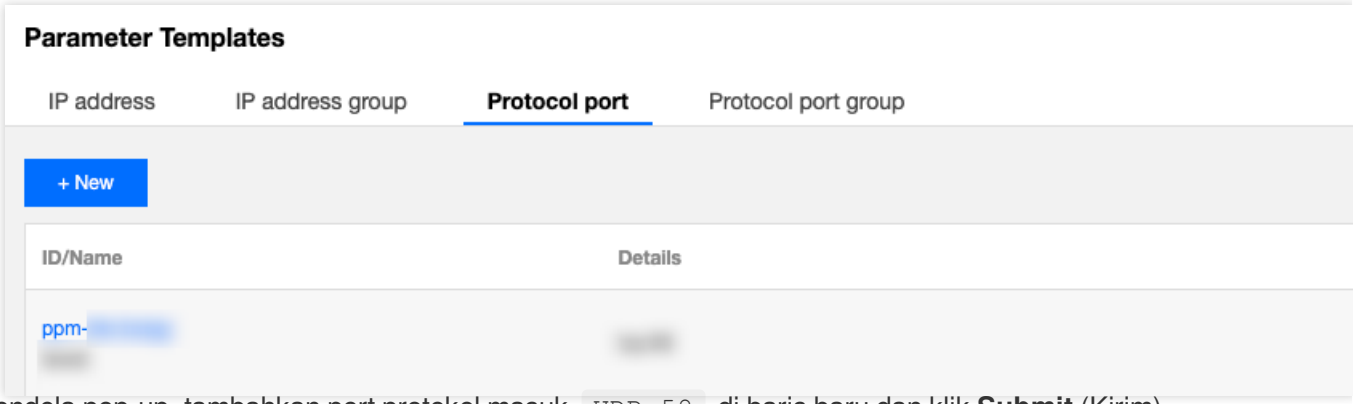
1. Pada tab **IP Address** (Alamat IP) templat parameter, cari templat parameter `ipm-0ge3ob8e` .
2. Klik **Edit** (Edit) di sebelah kanan.



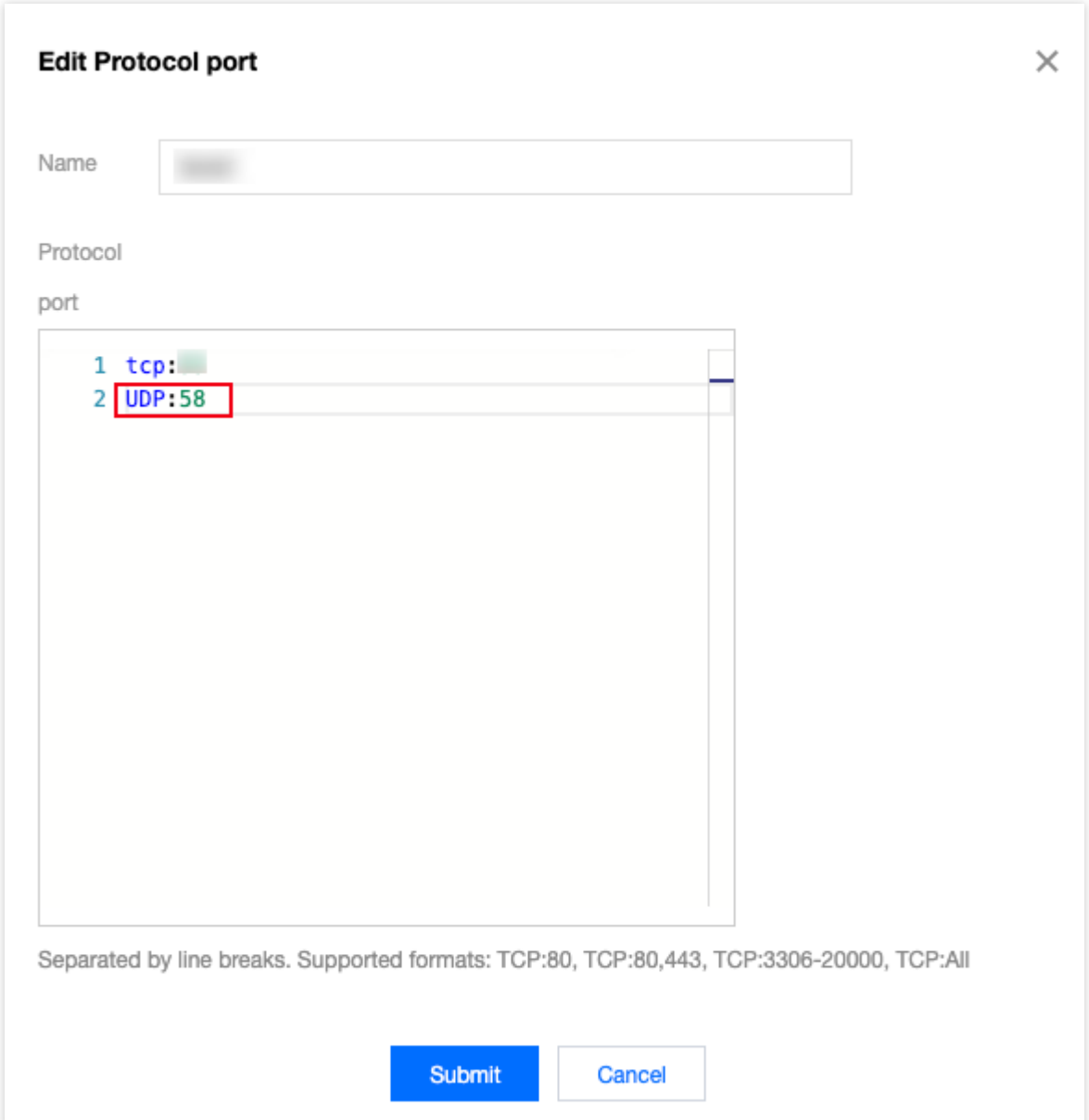
3. Di jendela pop-up, tambahkan rentang IP `10.0.1.0/27` di baris baru dan klik **Submit** (Kirim).



4. Pada tab **Protocol Port** (Port Protokol) pada templat parameter, cari templat parameter `ppm-4ty1ck3i` .
5. Klik **Edit** (Edit) di sebelah kanan.



6. Di jendela pop-up, tambahkan port protokol masuk `UDP:58` di baris baru dan klik **Submit** (Kirim).



Manajemen Akses

Ikhtisar Manajemen Akses Cloud

Waktu update terbaru：2024-01-24 17:55:51

Jika Anda menggunakan beberapa layanan Tencent Cloud seperti VPC, CVM, dan TencentDB yang dikelola oleh pengguna berbeda yang membagikan kunci akun Tencent Cloud Anda, Anda mungkin mengalami masalah berikut:
Kunci Anda dibagikan oleh beberapa pengguna, sehingga berisiko tinggi mengalami kebocoran.
Anda tidak dapat membatasi izin akses pengguna lain yang menimbulkan risiko keamanan karena potensi kesalahan operasi.
Untuk mencegah masalah ini, sebaiknya gunakan sub-akun untuk mengizinkan pengguna yang berbeda mengelola layanan yang berbeda. Secara default, sub-akun tidak memiliki izin untuk menggunakan sumber daya terkait CVM atau CVM. Dengan demikian, Anda perlu membuat kebijakan untuk memberikan sumber daya atau izin yang diperlukan ke sub-akun.

Ikhtisar

Tencent Cloud menyediakan layanan web yang disebut Cloud Access Management (CAM) untuk membantu pelanggan mengelola akses ke sumber dayanya dengan aman menggunakan akun Tencent Cloud mereka. Anda dapat menggunakan CAM untuk membuat, mengelola, dan menghentikan pengguna (atau grup pengguna), serta menggunakan manajemen identitas dan manajemen kebijakan untuk mengontrol sumber daya Tencent Cloud yang dapat digunakan oleh setiap pengguna.
Saat menggunakan CAM, Anda dapat menghubungkan kebijakan ke pengguna atau grup pengguna. Kebijakan dapat mengizinkan atau menolak permintaan pengguna untuk menggunakan sumber daya tertentu guna menyelesaikan tugas tertentu.
Untuk mengetahui informasi selengkapnya tentang kebijakan CAM, lihat Sintaksis Kebijakan.
Untuk mengetahui informasi selengkapnya tentang cara menggunakan kebijakan CAM, lihat Kebijakan.
Jika tidak perlu mengelola izin akses sub-akun untuk sumber daya VPC, Anda dapat melewati bagian ini. Ini tidak akan memengaruhi pemahaman Anda dan penggunaan bagian lain dalam dokumen.

Memulai

Kebijakan CAM harus mengizinkan atau menolak penggunaan satu atau beberapa operasi VPC. Pada saat yang sama, kebijakan ini harus menentukan sumber daya (yang dapat berupa semua sumber daya atau sebagian sumber daya untuk operasi tertentu) yang dapat digunakan untuk operasi tersebut. Kebijakan juga dapat mencakup ketentuan yang ditetapkan untuk sumber daya operasi.

Beberapa operasi VPC API mendukung izin tingkat sumber daya. Artinya, saat memanggil API ini, Anda tidak dapat menentukan beberapa sumber daya untuk operasi tersebut. Sebaliknya, Anda harus menentukan semua sumber daya untuk operasi.

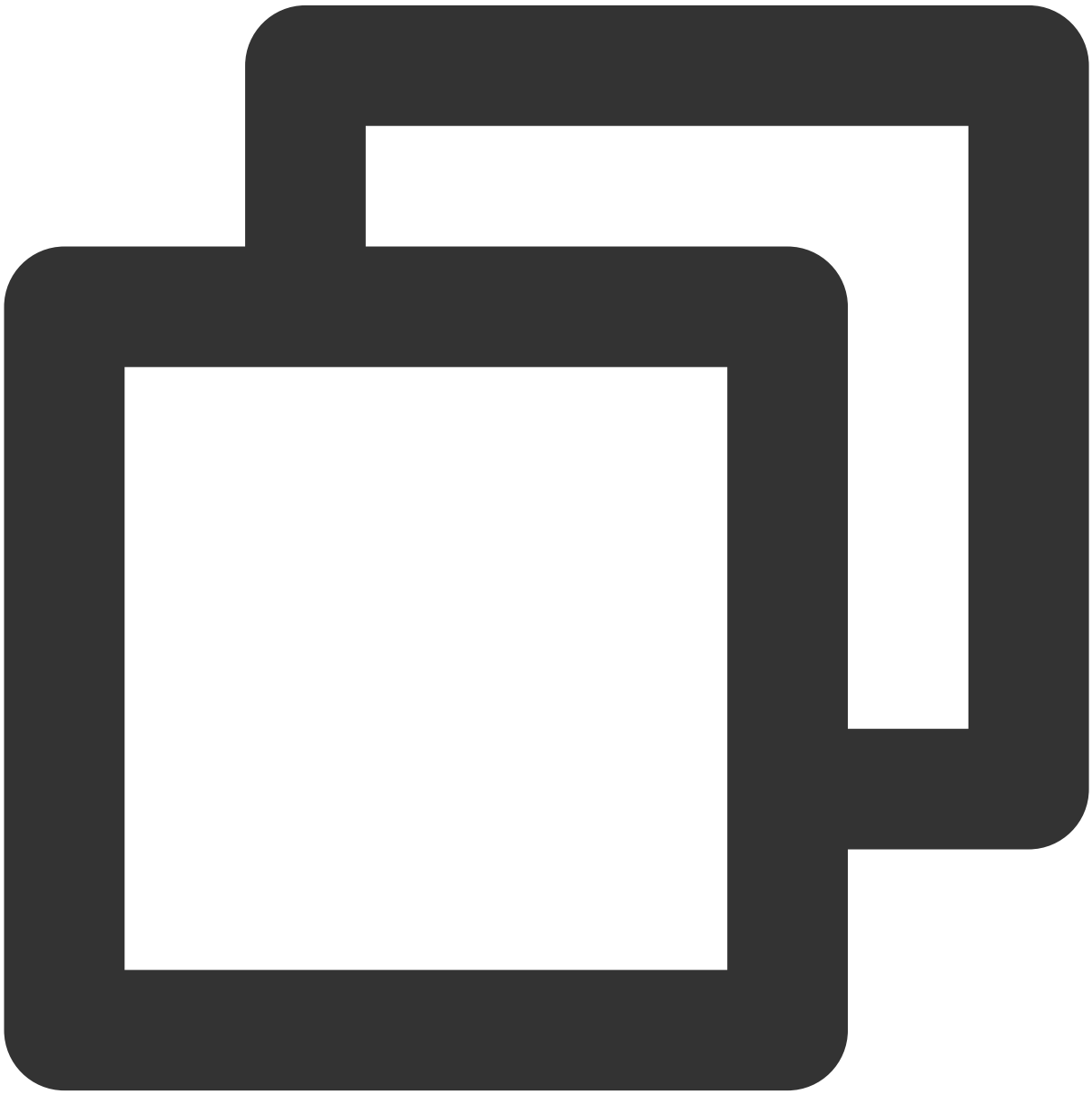
Tugas	Tautan
Struktur dasar suatu kebijakan	Sintaksis Kebijakan
Menentukan operasi dalam kebijakan	Operasi VPC
Menentukan sumber daya dalam kebijakan	Jalur Sumber Daya VPC
Izin tingkat sumber daya yang didukung oleh VPC	Izin Tingkat Sumber Daya yang Didukung oleh VPC
Sampel konsol	Sampel Konsol

Jenis Sumber Informasi yang Dapat Diotorisasi

Waktu update terbaru：2024-01-24 17:55:51

Sintaksis Kebijakan

Kebijakan CAM:



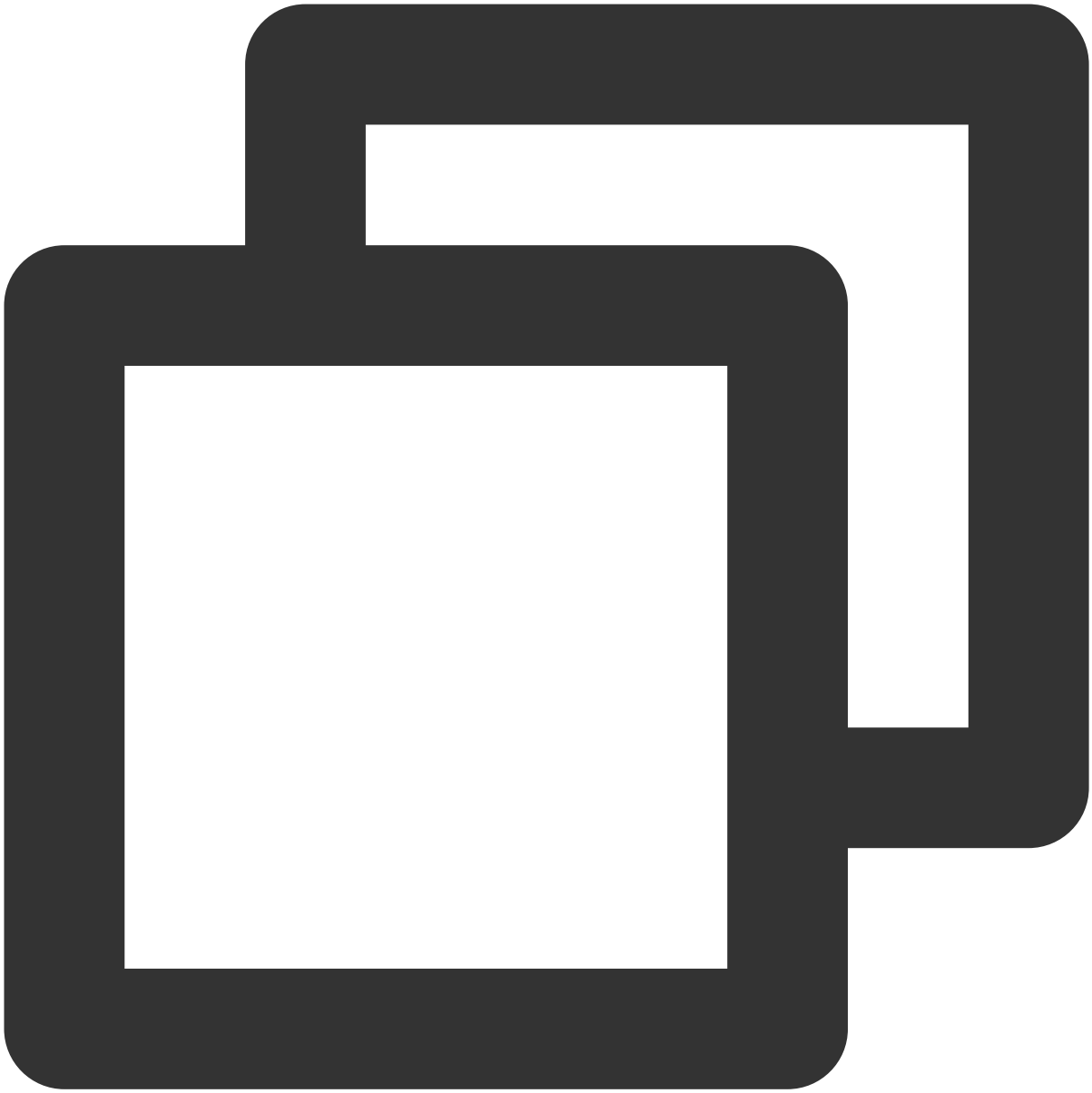
```
{
```

```
          "version":"2.0",
          "statement":
          [
              {
                  "effect":"effect",
                  "action":["action"],
                  "resource":["resource"],
                   "condition": {"key":{"value"}}
              }
          ]
}
```

version (versi) diperlukan. Saat ini, hanya nilai "2.0" yang diizinkan.
statement (pernyataan) menjelaskan detail dari satu atau beberapa izin. Elemen ini berisi izin atau sekumpulan izin yang terdiri dari elemen lain seperti efek, tindakan, sumber daya, dan ketentuan. Setiap kebijakan memiliki satu elemen pernyataan.
1.1 **action** (tindakan) menjelaskan tindakan yang diizinkan atau ditolak. Suatu tindakan dapat berupa API (dijelaskan menggunakan awalan "name") atau kumpulan fitur (satu kumpulan API tertentu, dijelaskan menggunakan awalan "permid"). Elemen ini diperlukan.
1.2 **resource** (sumber daya) menjelaskan detail otorisasi. Sumber daya dijelaskan dalam format enam bagian. Definisi sumber daya terperinci berbeda-beda tergantung produk. Untuk informasi selengkapnya tentang cara menentukan sumber daya, lihat dokumentasi untuk produk dengan sumber daya yang pernyataannya ditulis. Elemen ini diperlukan.
1.3 **condition** (kondisi) menjelaskan kondisi agar kebijakan diterapkan. Kondisi terdiri dari operator, kunci tindakan, dan nilai tindakan. Nilai kondisi dapat berisi informasi seperti waktu dan alamat IP. Beberapa layanan mengizinkan Anda untuk menentukan nilai tambahan dalam suatu kondisi. Elemen ini opsional.
1.4 **effect** (efek) menjelaskan apakah hasil yang dibuat oleh pernyataan tersebut "allowed" (diizinkan) atau "denied" (ditolak). Elemen ini diperlukan.

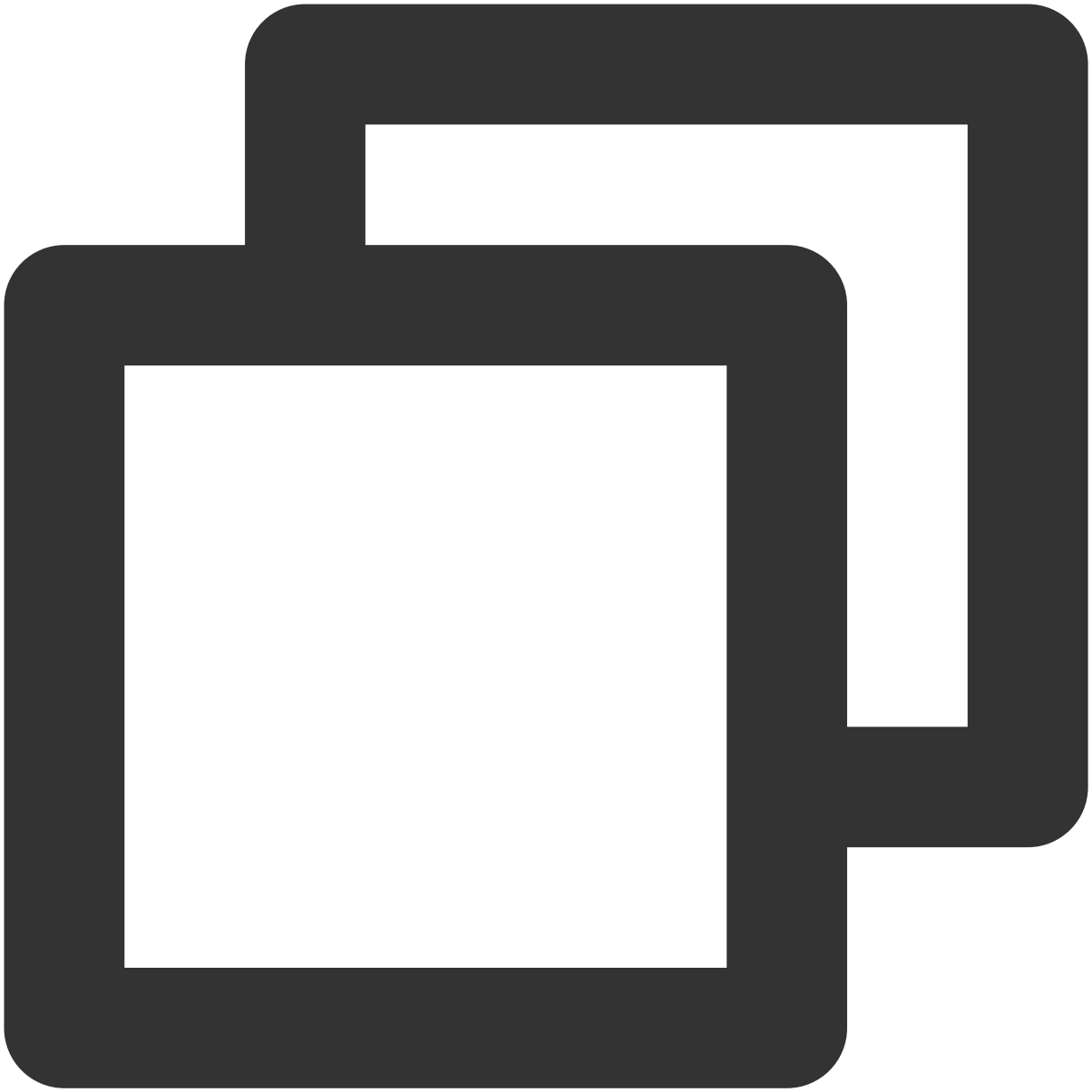
Operasi VPC

Dalam pernyataan kebijakan CAM, Anda dapat menentukan tindakan API apa pun dari layanan yang mendukung CAM. Untuk VPC, gunakan API dengan awalan "name/vpc:", misalnya name/vpc:Describe atau name/vpc:CreateRoute.
Untuk menentukan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma, seperti yang ditunjukkan di bawah ini:



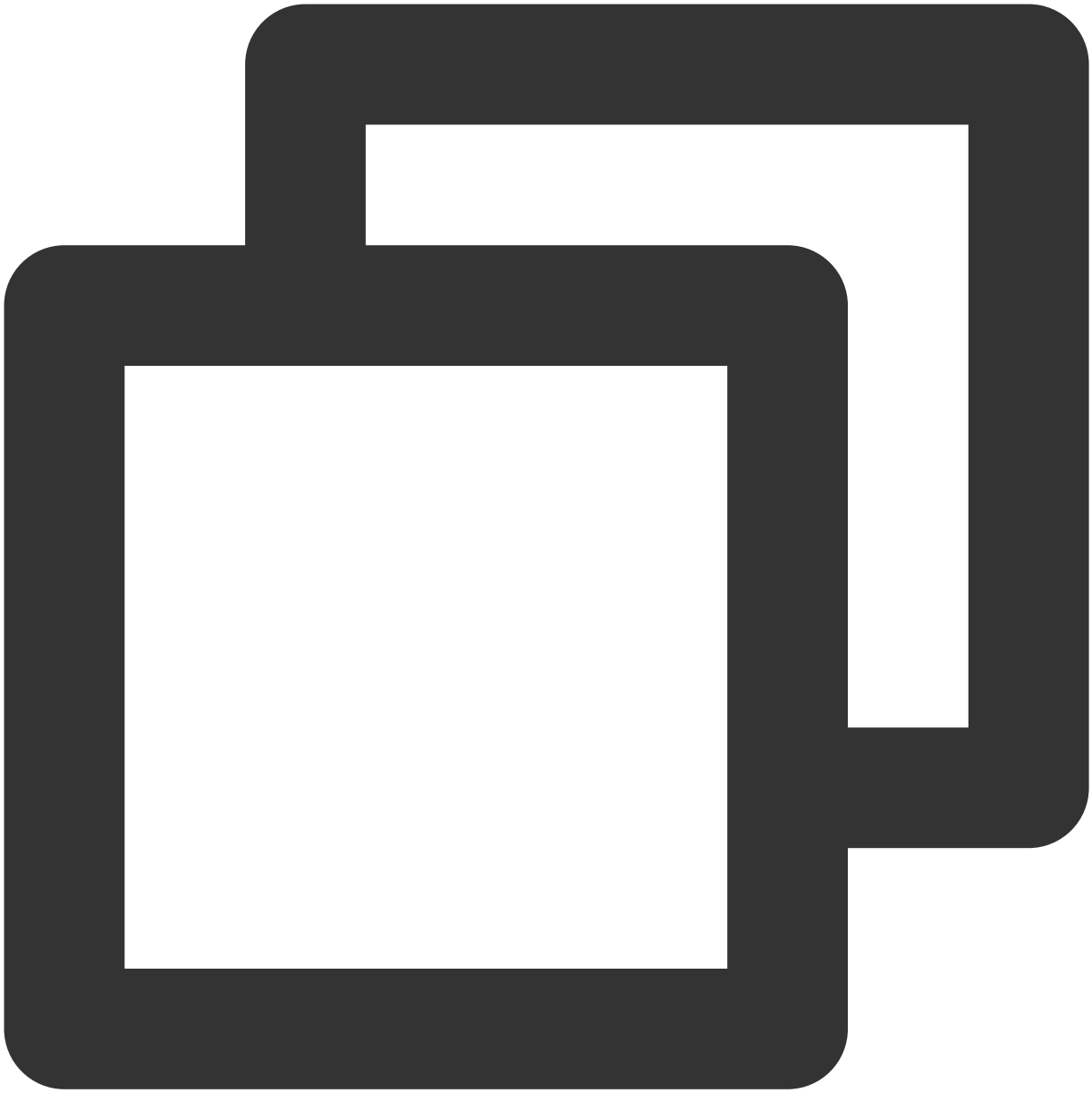
```
"action":["name/cvm:action1","name/cvm:action2"]
```

Anda juga dapat menentukan beberapa tindakan menggunakan karakter wildcard. Misalnya, Anda dapat menentukan semua API yang namanya dimulai dengan "Describe", seperti yang ditunjukkan di bawah ini:



```
"action":["name/cvm:Describe*"]
```

Untuk menentukan semua tindakan di VPC, gunakan karakter wildcard "*" sebagai berikut:

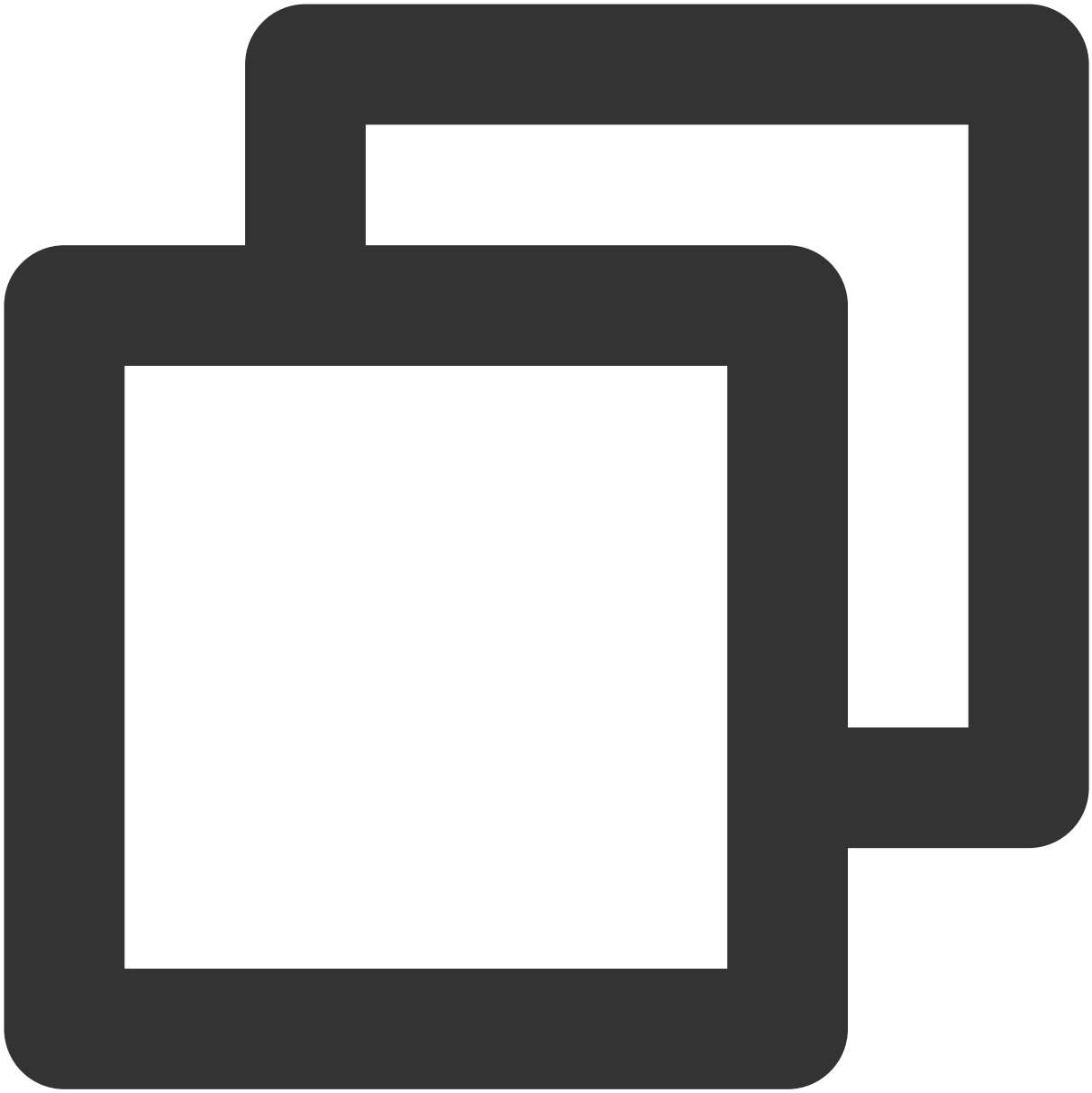


```
"action": ["name/cvm:*"]
```

Jalur Sumber Daya VPC

Setiap pernyataan kebijakan CAM memiliki sumber dayanya sendiri.

Format umum jalur sumber daya adalah sebagai berikut:



```
****qcs**:project_id:service_type:region:account:resource**
```

project_id: informasi proyek. Elemen ini hanya digunakan untuk mengaktifkan kompatibilitas dengan logika CAM lama dan dapat dibiarkan kosong.

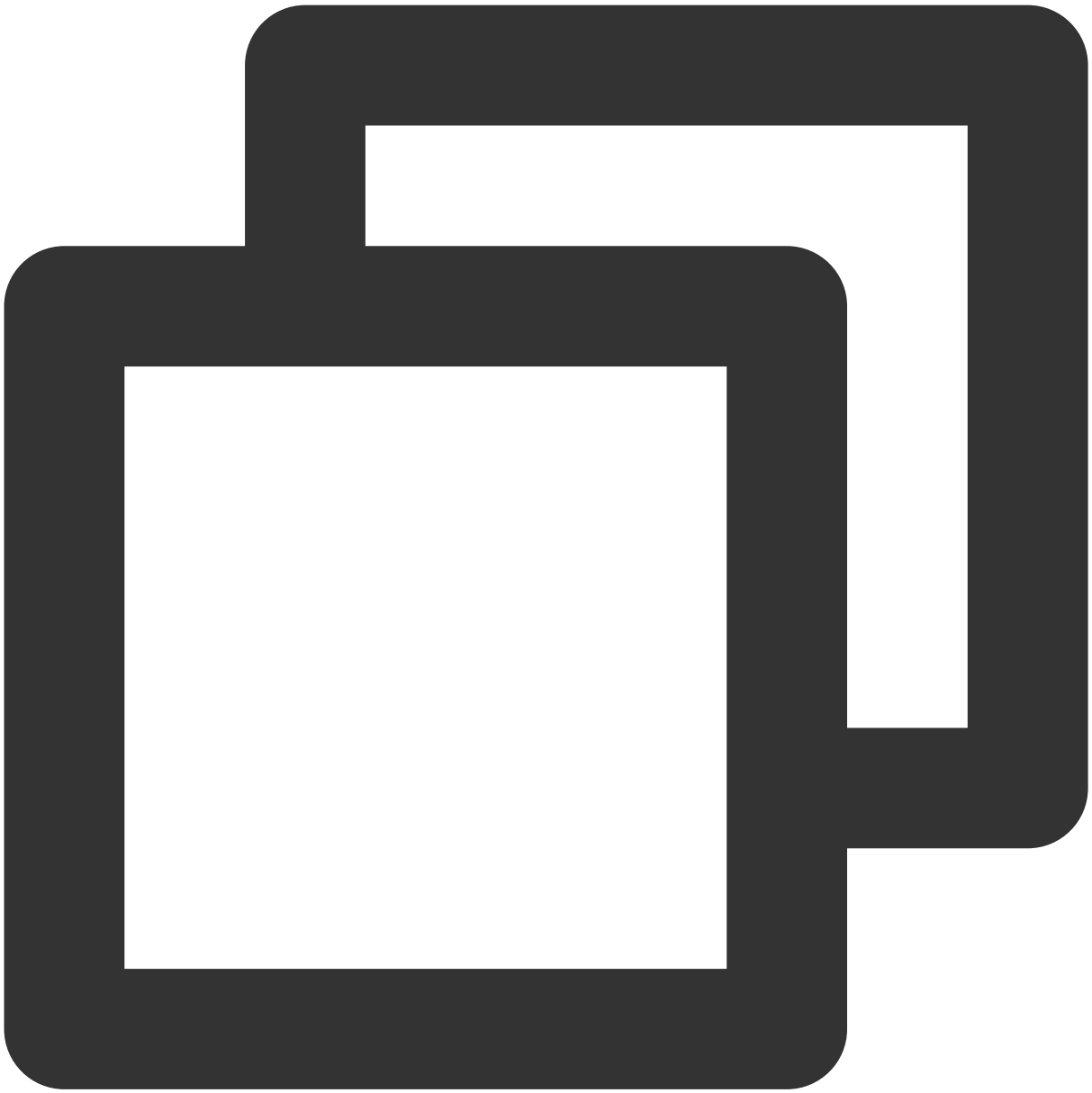
service_type: singkatan dari produk, seperti CVM.

region (wilayah): informasi wilayah, seperti bj.

account (akun): akun dari pemilik sumber daya, seperti uin/164256472.

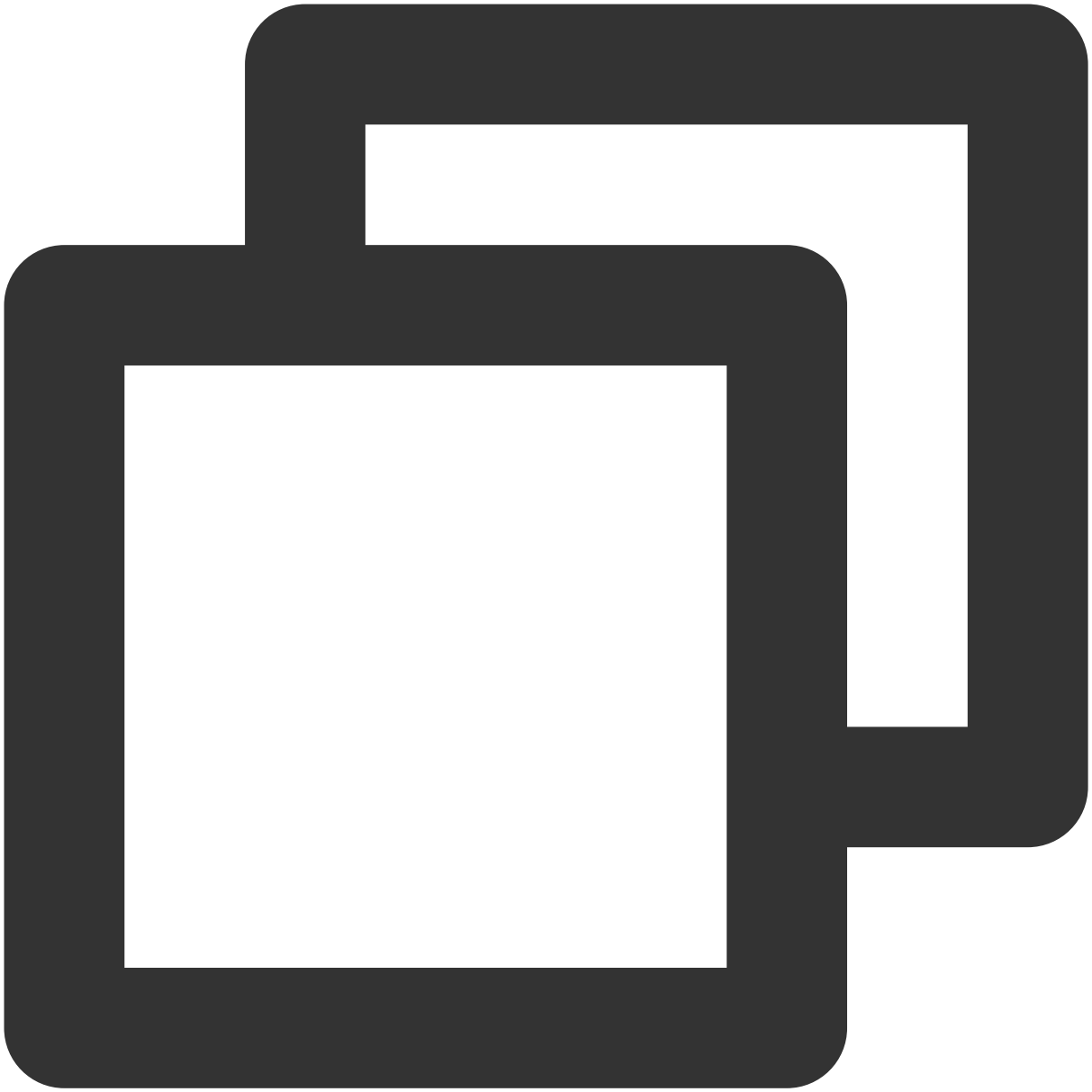
resource (sumber daya): detail sumber daya setiap produk, seperti vpc/vpc_id1 atau vpc/*.

Misalnya, Anda dapat menentukan instans (vpc-d08sl2zr dalam kasus ini) dalam pernyataan, seperti yang ditunjukkan di bawah ini:



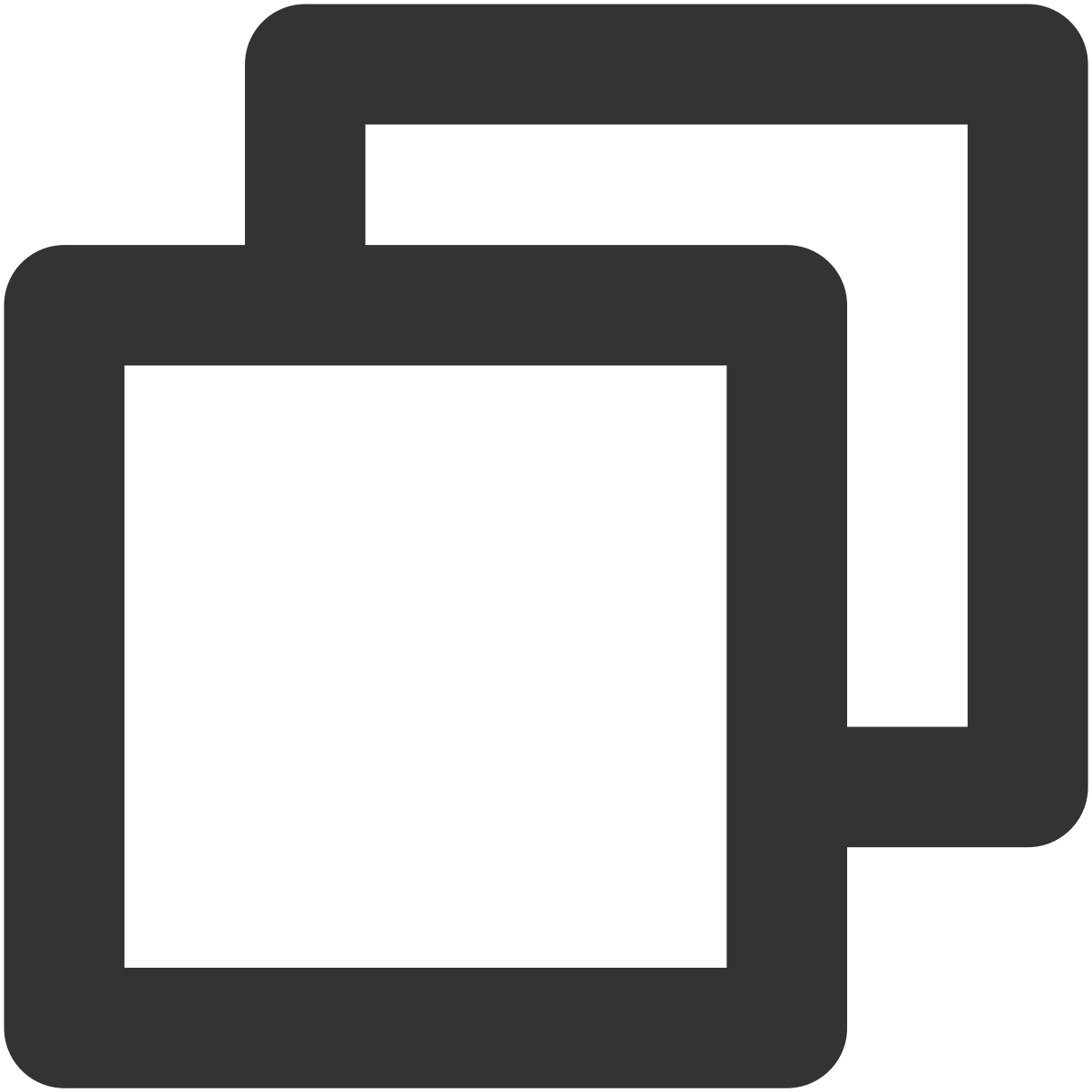
```
"resource":[ "qcs::vpc:bj:uin/164256472:instance/vpc-d08sl2zr"]
```

Anda juga dapat menggunakan karakter wildcard "*" untuk menentukan semua instans milik akun tertentu seperti yang ditunjukkan di bawah ini:



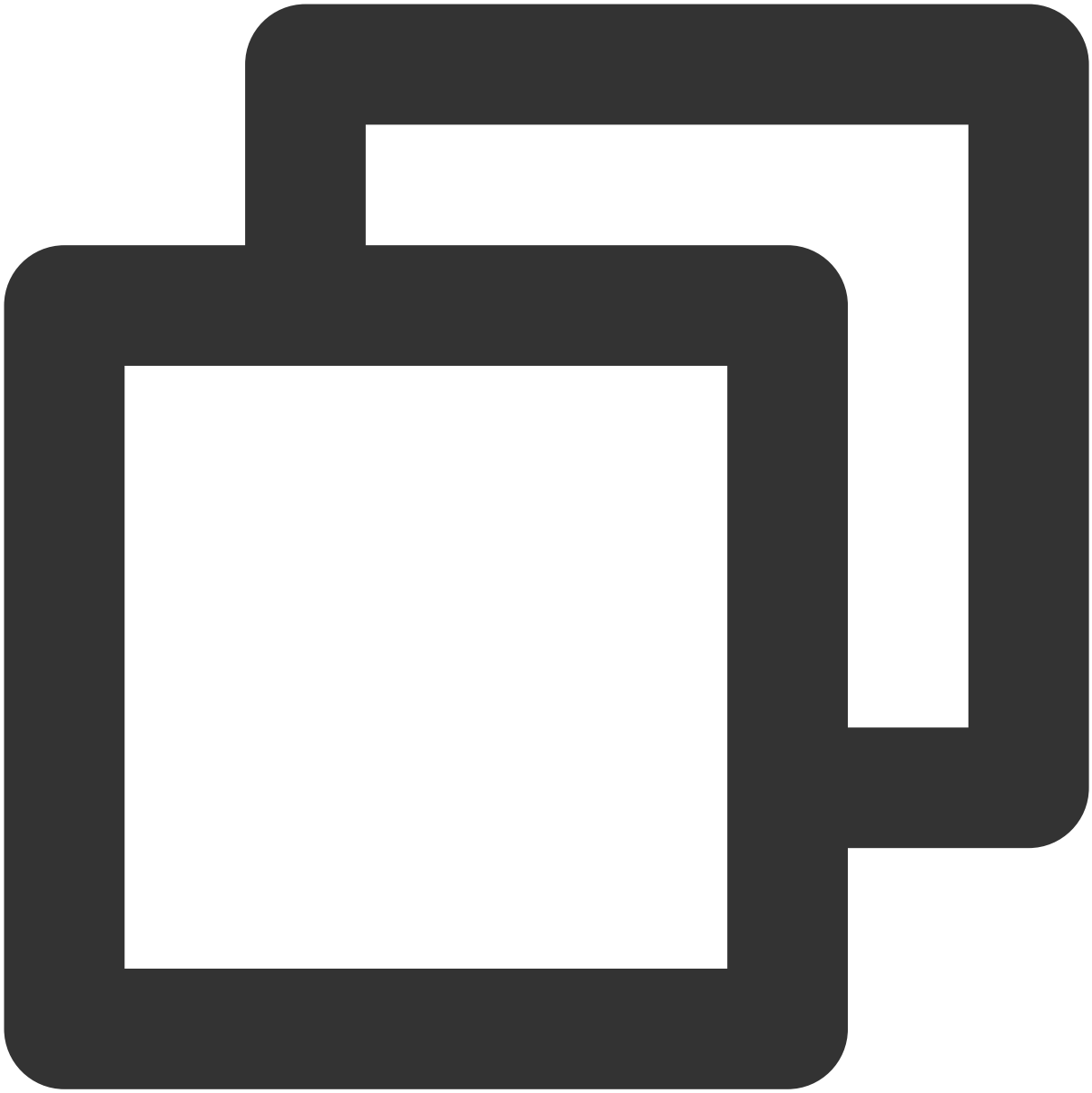
```
"resource":[ "qcs::redis:bj:uin/164256472:instance/*"]
```

Untuk menentukan semua sumber daya atau jika operasi API yang tidak mendukung izin tingkat sumber daya, Anda dapat menggunakan karakter wildcard "*" di `resource` seperti yang ditunjukkan di bawah ini:



```
"resource":["*"]
```

Untuk menentukan beberapa sumber daya dalam satu instruksi, pisahkan dengan koma. Dalam contoh berikut, dua sumber daya ditentukan:



```
"resource":["resource1","resource2"]
```

Tabel berikut menjelaskan sumber daya yang bisa digunakan VPC dan metode terkait untuk mendeskripsikan sumber daya ini.

Dalam tabel berikut, kata-kata berawalan "$" adalah semua nama alternatif.

`project` menunjukkan ID proyek.

`region` menunjukkan wilayah.

`account` menunjukkan ID akun.

Sumber Daya	Metode Deskripsi Sumber Daya dalam Kebijakan Otorisasi

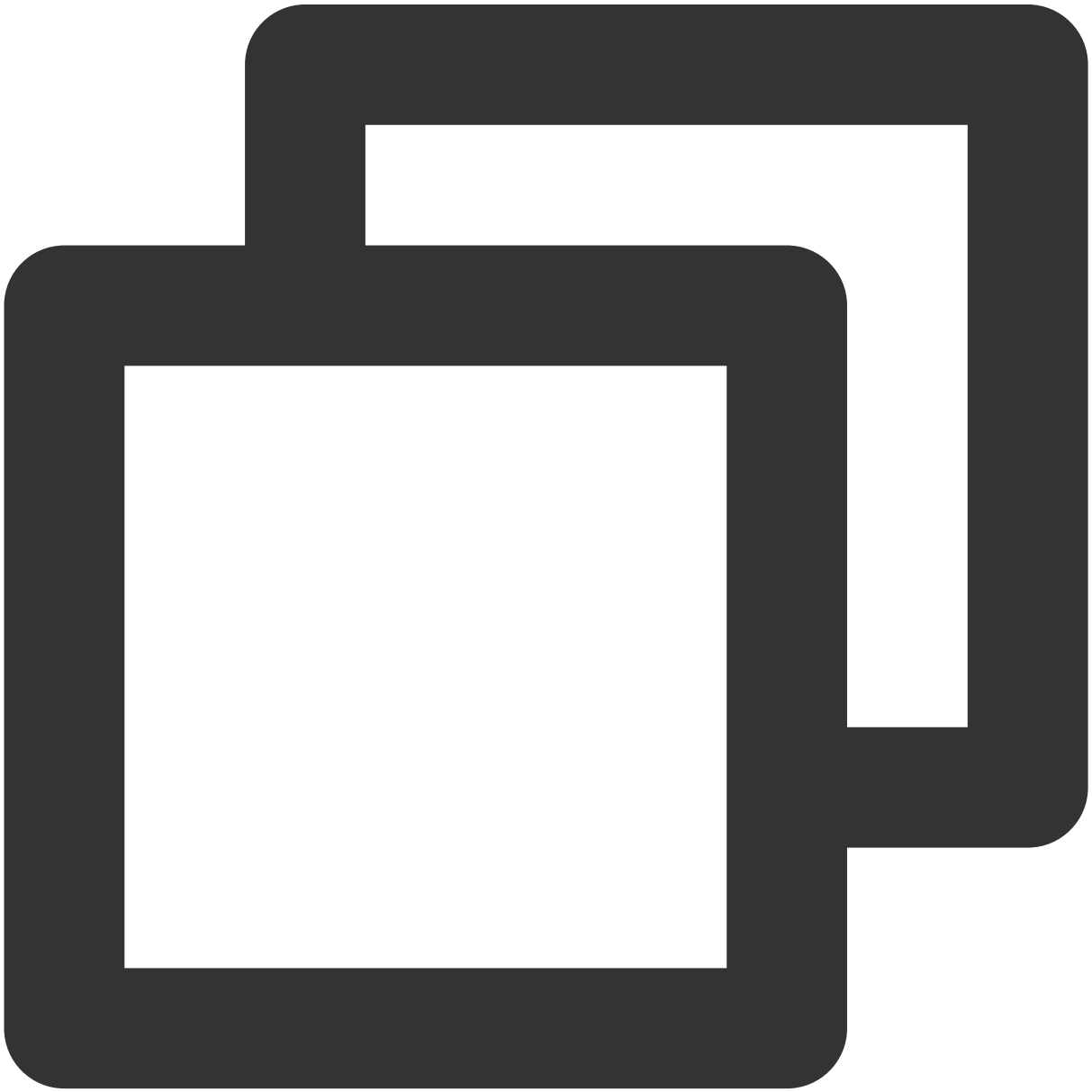
VPC	qcs::vpc:$region:$account:vpc/$vpcId
Subnet	qcs::vpc:$region:$account:subnet/$subnetId
Grup keamanan	qcs::cvm:$region:$account:sg/$sgId
EIP	qcs::cvm:$region:$account:eip/*

Contoh Kebijakan Manajemen Akses VPC

Waktu update terbaru：2024-01-24 17:55:51

Kebijakan Izin Baca-tulis Penuh untuk VPC

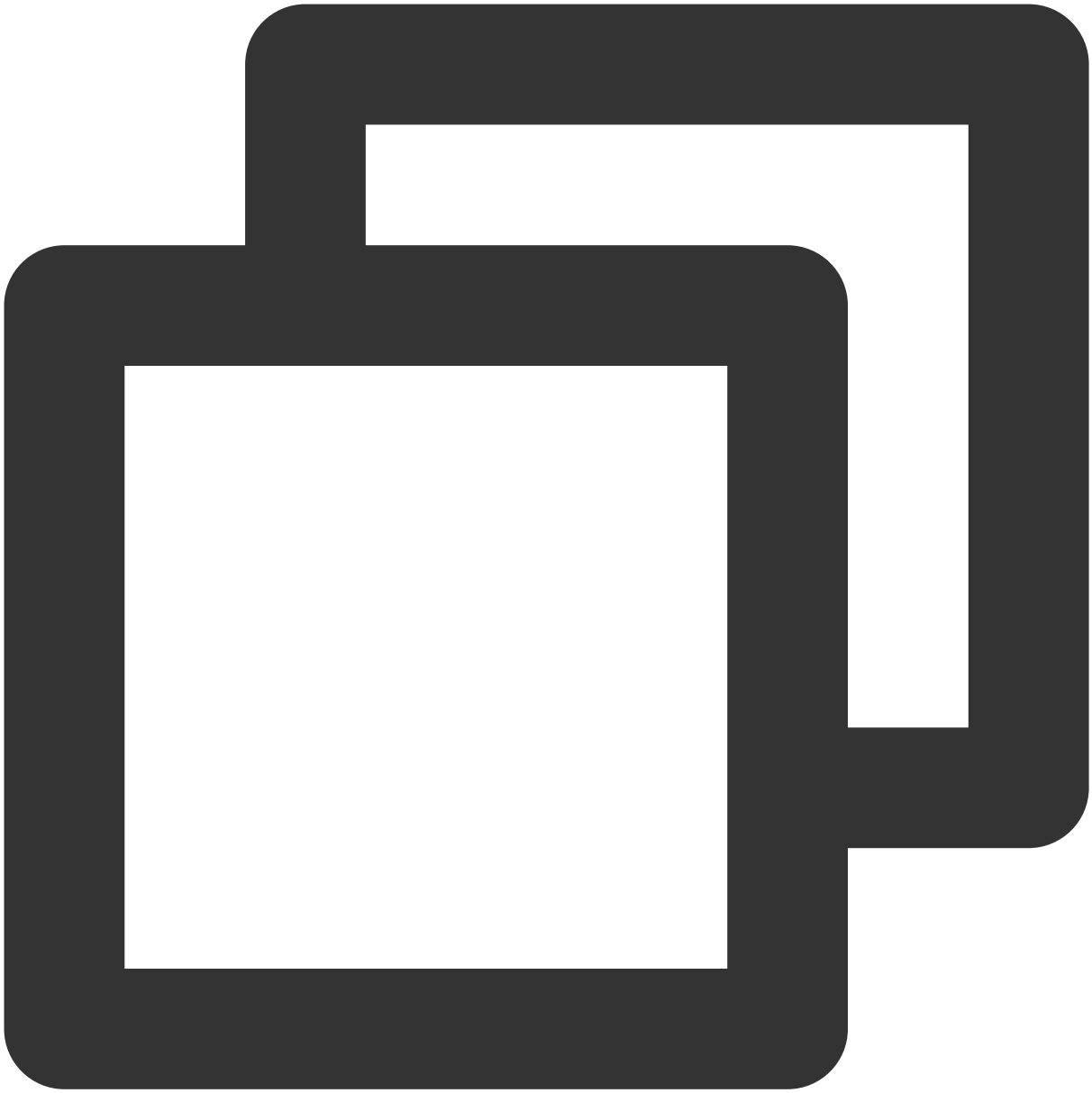
Kebijakan berikut mengizinkan Anda membuat dan mengelola instans VPC. Anda dapat menghubungkan kebijakan ini dengan sekelompok admin jaringan. Elemen `Action` menentukan semua API terkait VPC.



```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

Kebijakan Izin Baca Saja untuk VPC

Kebijakan berikut mengizinkan Anda mengkueri VPC Anda dan sumber daya yang relevan. Namun, Anda tidak dapat membuat, memperbarui, atau menghapusnya dengan kebijakan ini.
Sebaiknya berikan izin baca-saja VPC untuk pengguna, karena pengguna harus dapat melihat sumber daya untuk mengoperasikannya di konsol.

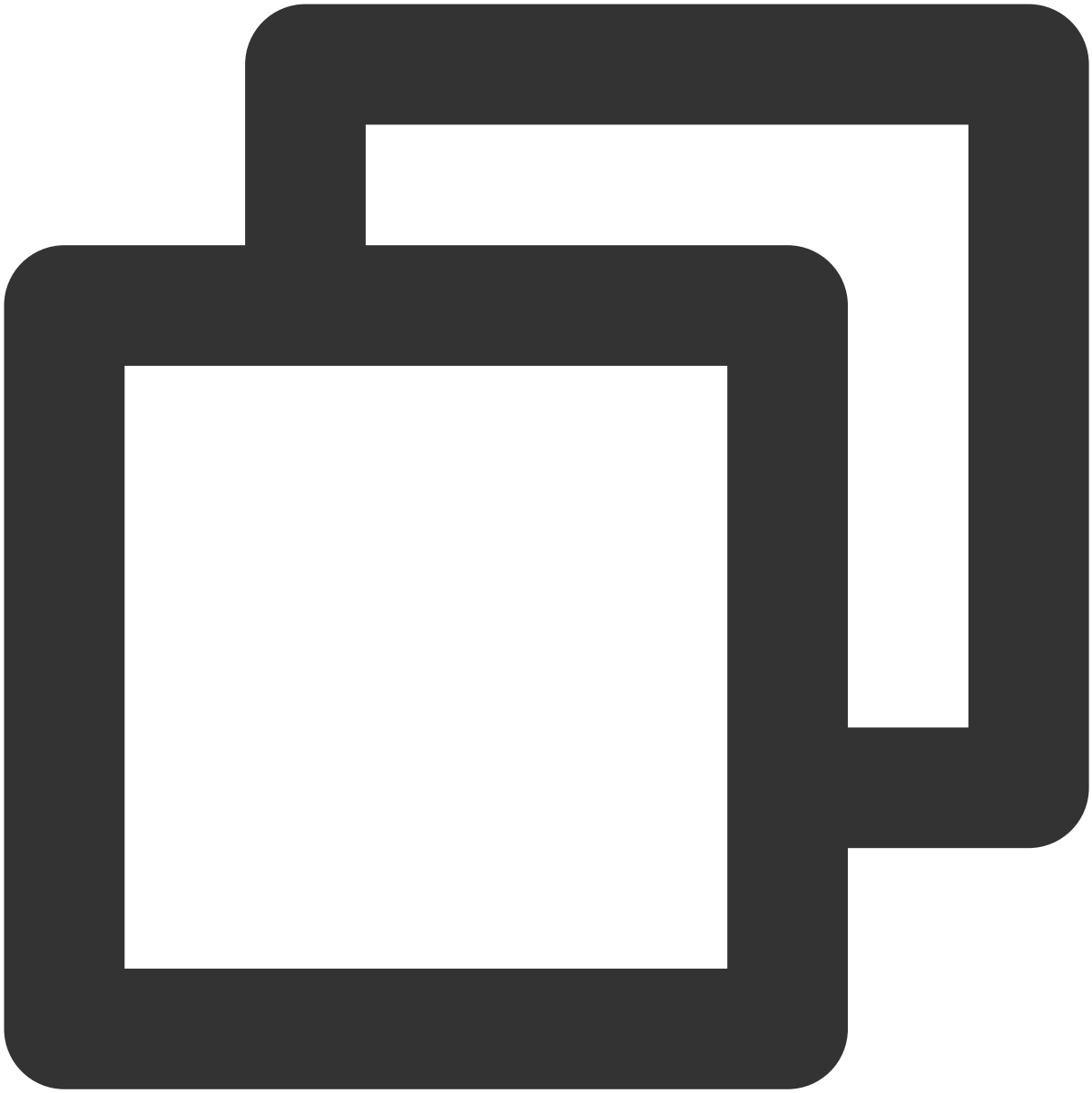


```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:Describe*",
                "name/vpc:Inquiry*",
                "name/vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
```

```
            }
        ]
}
```

Mengizinkan Sub-Akun untuk Mengelola VPC Tunggal Saja

Kebijakan berikut mengizinkan pengguna untuk melihat semua instans VPC tetapi hanya dapat mengoperasikan VPC A (misalnya, VPC A dengan ID vpc-d08sl2zr) dan sumber daya jaringan di VPC A (seperti subnet dan tabel rute, tetapi tidak termasuk komputer virtual cloud (CVM) dan database). Dengan kata lain, pengguna tidak diizinkan untuk mengelola instans VPC lainnya.
Versi ini tidak mendukung **allowing the user to view VPC A only** (mengizinkan pengguna melihat VPC A saja) yang akan didukung di versi mendatang.

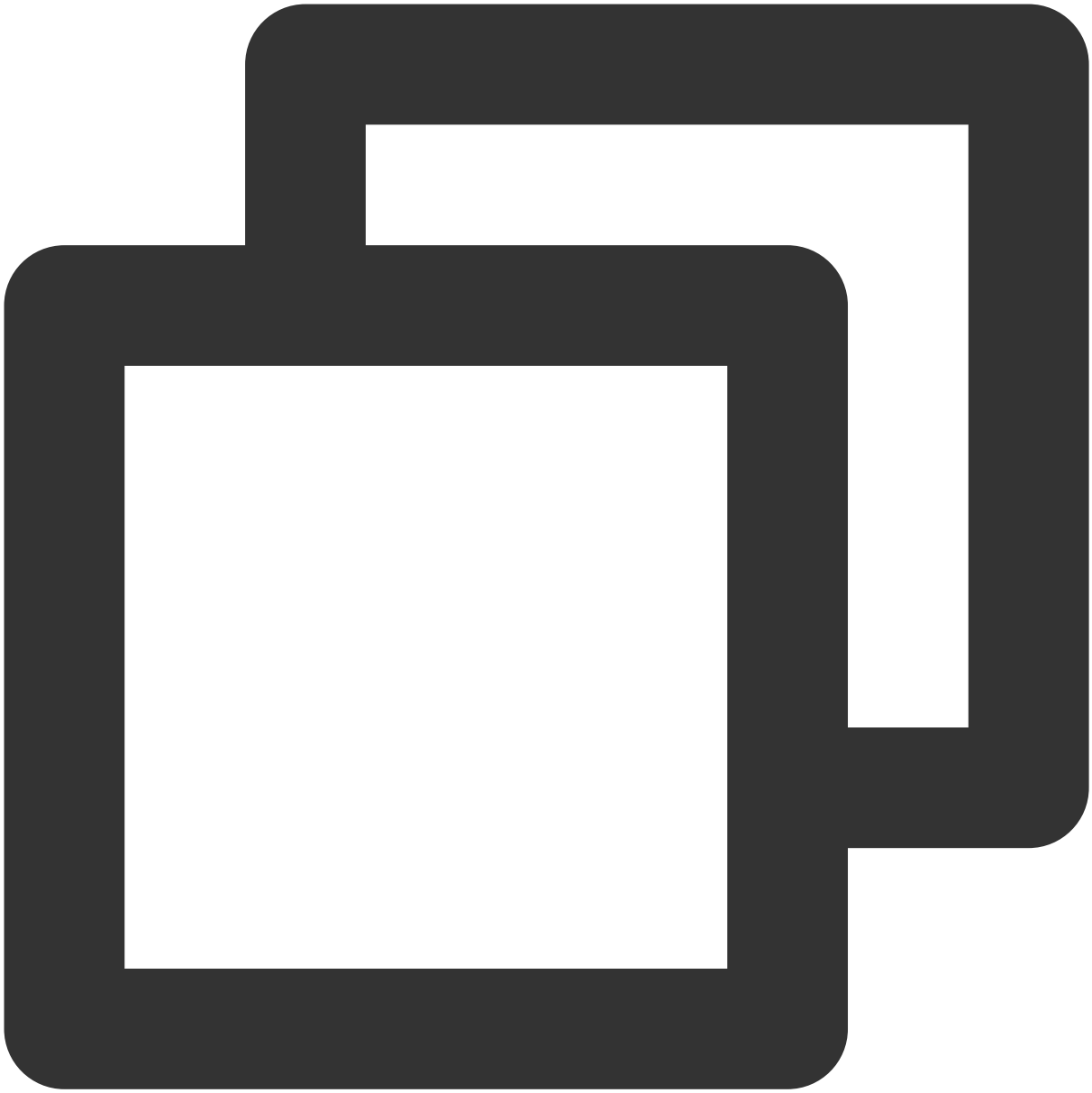


```
{
    "version": "2.0",
    "statement": [
        {
            "action": "name/vpc:*",
            "resource": "*",
            "effect": "allow",
            "condition": {
                "string_equal_if_exist": {  //Conditional judgment: hanya instans y
                    "vpc:vpc": [
                    "vpc-d08sl2zr"
```

```
                    ],
                    "vpc:accepter_vpc": [
                     "vpc-d08sl2zr"
                    ],
                     "vpc:requester_vpc": [
                     "vpc-d08sl2zr"
                    ]
                }
            }
        }
    ]
}
```

Mengizinkan Pengguna Mengelola Instans VPC tetapi Tidak Mengoperasikan Tabel Rute

Kebijakan berikut mengizinkan pengguna untuk membaca dan menulis instans VPC dan sumber daya yang relevan, tetapi tidak mengizinkan pengguna untuk mengoperasikan tabel rute.

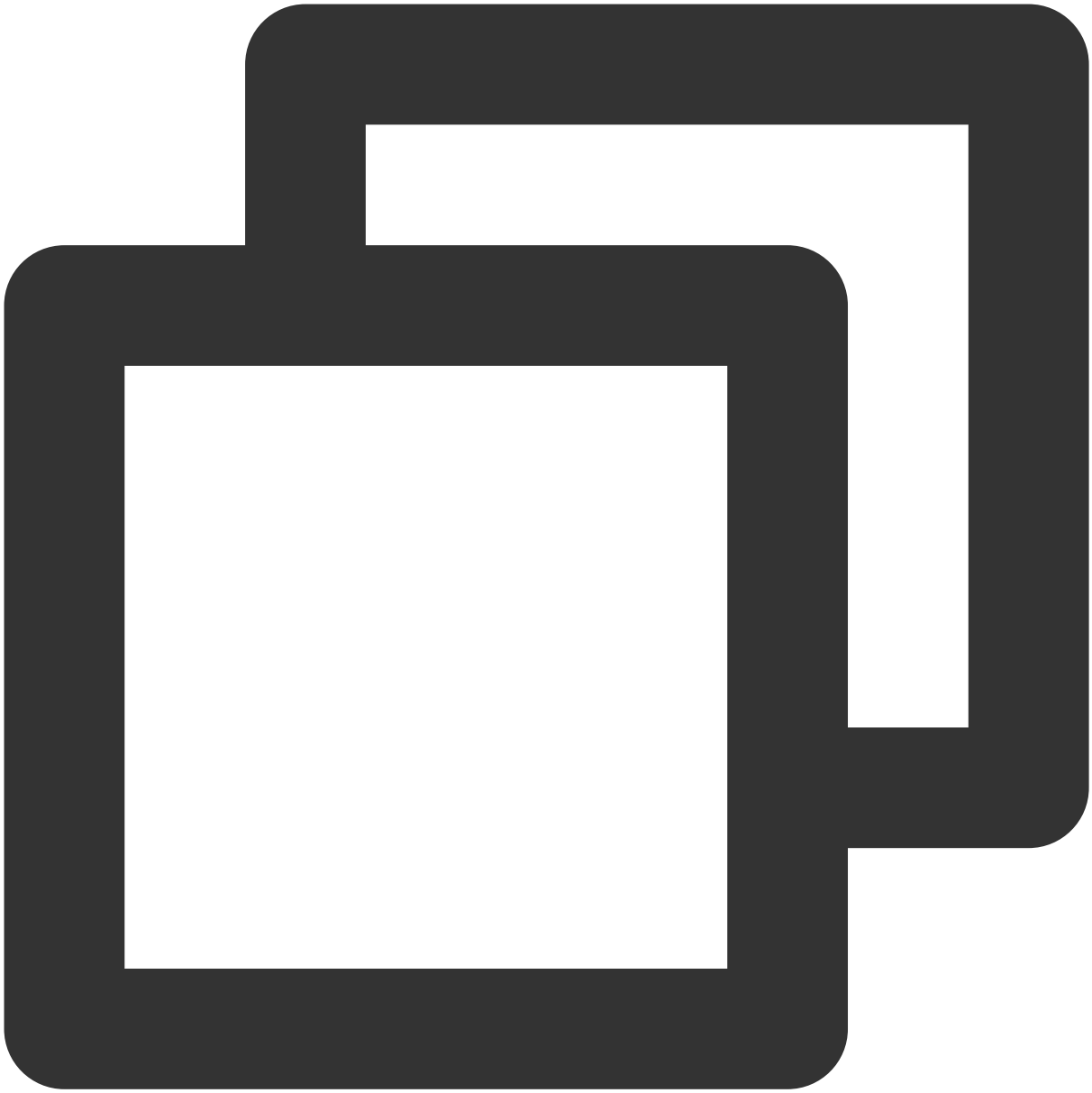


```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
```

```
            "action": [
                "name/vpc:AssociateRouteTable",
                "name/vpc:CreateRoute",
                "name/vpc:CreateRouteTable",
                "name/vpc:DeleteRoute",
                "name/vpc:DeleteRouteTable",
                "name/vpc:ModifyRouteTableAttribute"
            ],
            "resource": "*",
            "effect": "deny"
        }
    ]
}
```

Mengizinkan Pengguna Mengelola Sumber Daya VPN

Kebijakan berikut mengizinkan pengguna untuk melihat semua sumber daya VPC dan hanya mengizinkan pengguna untuk membuat, membaca, memperbarui, dan menghapus (CRUD) sumber daya VPN.



```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:Describe*",
                "name/vpc:Inquiry*",
                "name/vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
```

```
        },
        {
            "action": [
                "name/vpc:*Vpn*",
                "name/vpc:*UserGw*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

Izin Tingkat Sumber Informasi yang Didukung oleh VPC API

Waktu update terbaru：2024-01-24 17:55:51

Anda dapat mengotorisasi operasi API berikut untuk sumber daya VPC di CAM. Sumber daya yang didukung oleh API tertentu dan ketentuan yang terkait adalah sebagai berikut:

Keterangan:

Operasi VPC API yang tidak tercantum dalam tabel tidak mendukung izin tingkat sumber daya. Untuk melakukan operasi ini, Anda masih dapat mengotorisasi pengguna untuk melakukannya, tetapi Anda harus menetapkan `*` sebagai elemen sumber daya dalam pernyataan kebijakan.

Operasi API	Sumber daya
AcceptVpcPeeringConnection	Sumber daya VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
—	Sumber daya VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId (vpcId penerima)
AcceptVpcPeeringConnectionEx	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId

—	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
AddVpnConnEx	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya gateway VPN qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId
—	Sumber daya gateway pelanggan qcs::vpc:$region:$account:cgw/*
—	Sumber daya tunnel VPN qcs::vpc:$region:$account:vpnx/*
AssignPrivateIpAddresses	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
AssociateRouteTable	Sumber daya subnet qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId
—	Sumber daya tabel rute qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
AttachClassicLinkVpc	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya CVM

	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId
AttachNetworkInterface	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
—	Sumber daya CVM qcs::cvm:$region:$account:instance/* | Instans | qcs::cvm:$region:$account:instance/$instanceId |
CreateAndAttachNetworkInterface	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya CVM qcs::cvm:$region:$account:instance/* | Instans | qcs::cvm:$region:$account:instance/$instanceId |
—	Sumber daya ENI qcs::vpc:$region:$account:eni/*
CreateDirectConnectGateway	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/*
CreateLocalDestinationIPPortTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId

CreateLocalIPTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateLocalIPTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateLocalSourceIPPortTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateLocalSourceIPPortTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreatePeerIPTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateNatGateway	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya NAT gateway qcs::vpc:$region:$account:nat/*
CreateNetworkAcl	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya ACL jaringan qcs::vpc:$region:$account:acl/*
CreateNetworkInterface	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |

—	Sumber daya subnet | Subnet | qcs::vpc:$region:$account:vpc/$vpcId \| \| Subnet \| qcs::vpc:$region:$account:subnet/$subnetId |
—	Sumber daya ENI qcs::vpc:$region:$account:eni/*
CreateRoute	Sumber daya tabel rute qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
CreateRouteTable	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya tabel rute qcs::vpc:$region:$account:rtb/*
CreateSubnet	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya gateway subnet | Subnet | qcs::vpc:$region:$account:vpc/$vpcId |
CreateSubnetAclRule	Sumber daya ACL jaringan qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
—	Sumber daya gateway subnet | Subnet | qcs::vpc:$region:$account:vpc/$vpcId |

CreateVpcPeeringConnection	Sumber daya VPC (inisiator) qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/*
CreateVpcPeeringConnectionEx	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/*
DeleteDirectConnectGateway	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalDestinationIPPortTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalIPTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalIPTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/*

	qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalSourceIPPortTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeletePeerIPTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalSourceIPPortTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteNatGateway	Sumber daya NAT gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId
DeleteNetworkAcl	Sumber daya ACL jaringan qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
DeleteNetworkInterface	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
DeleteRoute	Sumber daya tabel rute qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
DeleteRouteTable	Sumber daya tabel rute qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId

DeleteSubnet	Sumber daya subnet | Subnet | qcs::vpc:$region:$account:vpc/$vpcId \| \| Subnet \| qcs::vpc:$region:$account:subnet/$subnetId |
DeleteUserGw	Sumber daya gateway pelanggan qcs::vpc:$region:$account:cgw/* qcs::vpc:$region:$account:cgw/$userGwId
DeleteVpc	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
DeleteVpcPeeringConnection	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
DeleteVpcPeeringConnectionEx	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
DeleteVpnConn	Sumber daya tunnel VPN qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId
DetachClassicLinkVpc	Sumber daya VPC

	qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya CVM qcs::cvm:$region:$account:instance/* | Instans | qcs::cvm:$region:$account:instance/$instanceId |
DetachNetworkInterface	Sumber daya CVM qcs::cvm:$region:$account:instance/* | Instans | qcs::cvm:$region:$account:instance/$instanceId |
—	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
DeteleSubnetAclRule	Sumber daya subnet | Subnet | qcs::vpc:$region:$account:vpc/$vpcId \| \| Subnet \| qcs::vpc:$region:$account:subnet/$subnetId |
—	Sumber daya ACL jaringan qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
EipBindNatGateway	Sumber daya NAT gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId
EipUnBindNatGateway	Sumber daya NAT gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId
EnableVpcPeeringConnection	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering

	qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
EnableVpcPeeringConnectionEx	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
MigrateNetworkInterface	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
—	Sumber daya CVM qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId(otorisasi diperlukan sebelum dan sesudah migrasi)
MigratePrivateIpAddress	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId

ModifyDirectConnectGateway	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalDestinationIPPortTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalIPTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalIPTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalSourceIPPortTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyPeerIPTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalSourceIPPortTranslationNatRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyNatGateway	Sumber daya NAT gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/nat-dc7cdf
ModifyNetworkAcl	Sumber daya ACL jaringan qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
ModifyNetworkAclEntry	Sumber daya ACL jaringan

	qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
ModifyNetworkInterface	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
ModifyPrivateIpAddress	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
ModifyRouteTableAttribute	Sumber daya tabel rute qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
ModifySubnetAttribute	Sumber daya subnet | Subnet | qcs::vpc:$region:$account:vpc/$vpcId \| \| Subnet \| qcs::vpc:$region:$account:subnet/$subnetId |
ModifyUserGw	Sumber daya gateway pelanggan qcs::vpc:$region:$account:cgw/* qcs::vpc:$region:$account:cgw/$userGwId
ModifyVpcAttribute	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
ModifyVpcPeeringConnection	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId

ModifyVpcPeeringConnectionEx	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
ModifyVpnConnEx	Sumber daya tunnel VPN qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId
ModifyVpnGw	Sumber daya gateway VPN qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId
RejectVpcPeeringConnection	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId

RejectVpcPeeringConnectionEx	Sumber daya VPC qcs::vpc:$region:$account:vpc/* | VPC | qcs::vpc:$region:$account:vpc/$vpcId |
—	Sumber daya koneksi peering qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
ResetVpnConnSA	Sumber daya tunnel VPN qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId
SetLocalIPTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
SetLocalSourceIPPortTranslationAclRule	Sumber daya gateway direct connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
SetSSLVpnDomain	Sumber daya gateway VPN qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId

UnassignPrivateIpAddresses	Sumber daya ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId

Alat Diagnostik
Probe Jaringan

Waktu update terbaru：2024-01-24 17:55:51

Layanan probe jaringan Tencent Cloud digunakan untuk memantau kualitas koneksi jaringan VPC, termasuk latensi, tingkat kehilangan paket, dan metrik kunci lainnya.
Dengan arsitektur jaringan cloud hibrida, Anda membuat probe jaringan di subnet yang perlu berkomunikasi dengan IDC Anda untuk memantau tingkat kehilangan paket dan latensi dari tautan yang di-probe. Konfigurasi memungkinkan Anda untuk:
Memantau kualitas koneksi
Menerima peringatan jika terjadi kegagalan koneksi

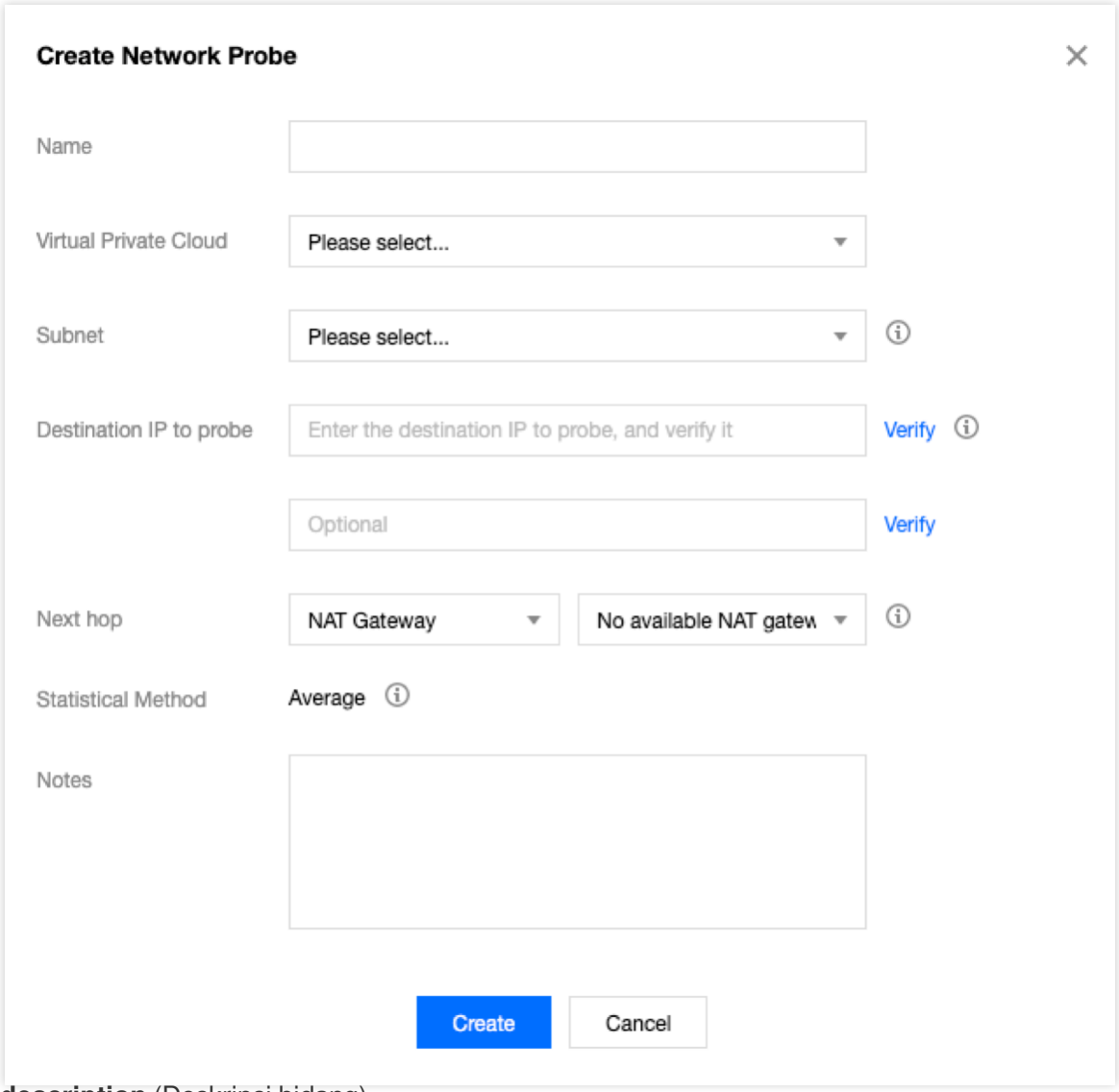
Petunjuk

Layanan probe jaringan mengadopsi metode ping dengan frekuensi 20 ping per menit.
Hingga 50 probe diperbolehkan untuk setiap VPC.
Maksimal 20 subnet di bawah VPC yang sama dapat memiliki probe jaringan.

Membuat Probe Jaringan

1. Login ke Konsol VPC.
2. Pilih **Diagnostic Tools** (Alat Diagnostik) -> **Network Probe** (Probe Jaringan) di bilah sisi kiri untuk masuk ke halaman pengelolaan.
3. Klik **+New** (+Baru) di bagian atas halaman **Network Probe** (Probe Jaringan).
4. Di jendela pop-up **Create Network Probe** (Buat Probe Jaringan), isi bidang yang relevan.

Keterangan:
Rute probe jaringan ditetapkan oleh sistem dan tidak dapat diubah.
Saat Anda mengganti rute subnet, rute default ini akan dihapus dari tabel rute asli yang terkait dengan subnet, dan ditambahkan ke tabel rute baru yang terkait.



Field description (Deskripsi bidang)

Bidang	Konfigurasi
Nama	Nama probe jaringan.
VPC	VPC tempat IP sumber probe berada.
Subnet	Subnet tempat IP sumber probe berada.
IP Tujuan Probe	Maksimal dua IP tujuan didukung untuk probe jaringan. Pastikan bahwa Anda telah mengaktifkan kebijakan firewall ICMP untuk server tujuan probe jaringan.
Sumber Hop Selanjutnya	Anda dapat memilih Tentukan atau Jangan Tentukan pada hop selanjutnya. Jika Jangan Tentukan dipilih, tidak ada hop selanjutnya yang akan dipilih. **Keterangan:** Do Not Specify (Jangan Tentukan) sekarang hanya tersedia untuk pengguna beta. Untuk mengaktifkannya, harap kirim tiket.

	Jika Anda menentukan hop selanjutnya, pilih jenis dan instans hop selanjutnya. Kemudian, sistem secara otomatis menambahkan rute 32-bit yang sesuai ke tabel rute terkait subnet. Saat ini, jenis hop selanjutnya yang didukung mencakup NAT Gateway, peering connection, VPN gateway, direct connect gateway, CVM, dan CCN. **Keterangan:** Jika Anda menentukan CCN sebagai hop selanjutnya dan IP tujuan probe menjadi milik dua VPC dalam CCN, rentang IP dengan mask terpanjang akan dicocokkan dan diterapkan.

5. (Opsional) **Verify** (Verifikasi) **Probe Destination IP** (IP Tujuan Probe)

Keterangan:

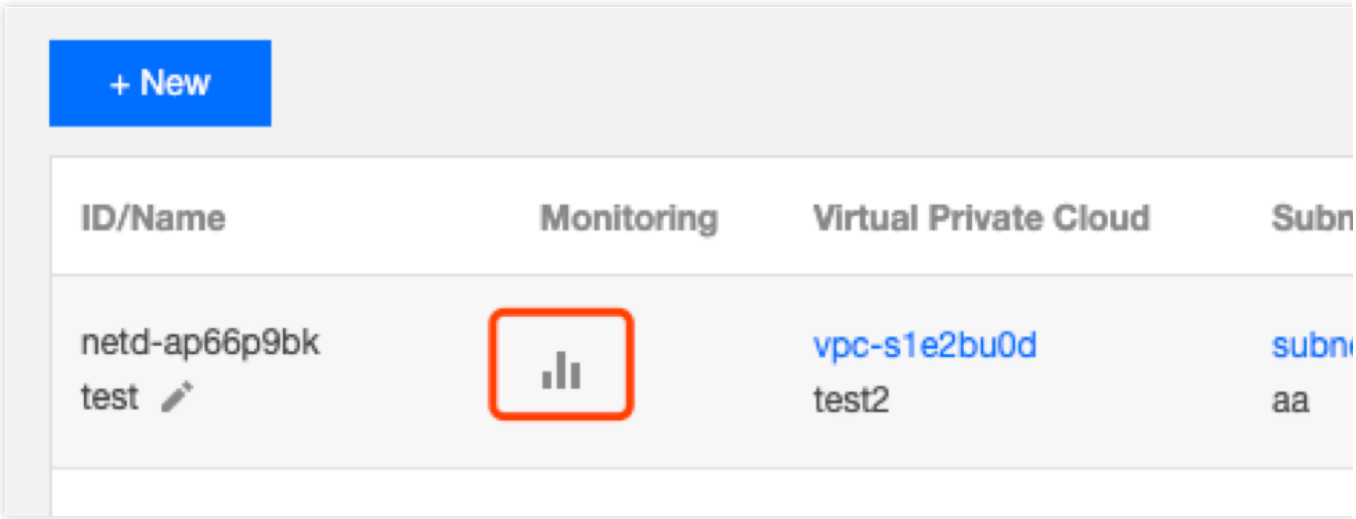
Lewati langkah ini jika Anda tidak menentukan hop selanjutnya.

Jika koneksi berhasil, klik **OK** (Oke).

Jika koneksi gagal, periksa apakah rute subnet dikonfigurasi dengan benar, dan apakah perangkat yang diperiksa mengaktifkan ACL Jaringan, grup keamanan, atau firewall lain, yang dapat memblokir koneksi. Untuk informasi selengkapnya, lihat Mengelola ACL Jaringan dan Memodifikasi Aturan Grup Keamanan.

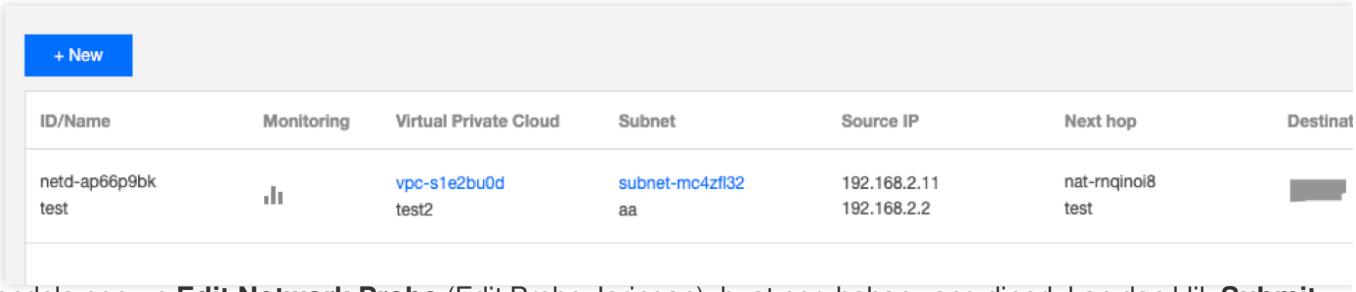
Memeriksa Latensi dan Paket Hilang dari Probe Jaringan

1. Login ke Konsol VPC.
2. Pilih **Diagnostic Tools** (Alat Diagnostik) -> **Network Probe** (Probe Jaringan) di bilah sisi kiri untuk masuk ke halaman pengelolaan.
3. Klik ikon pemantauan instans probe jaringan target untuk melihat latensi dan tingkat kehilangan paketnya.



Memodifikasi Probe Jaringan

1. Login ke Konsol VPC.
2. Pilih **Diagnostic Tools** (Alat Diagnostik) -> **Network Probe** (Probe Jaringan) di bilah sisi kiri untuk masuk ke halaman pengelolaan.
3. Dalam daftar, cari probe jaringan yang akan diubah dan klik **Edit** (Edit) di kolom **Operation** (Operasi).



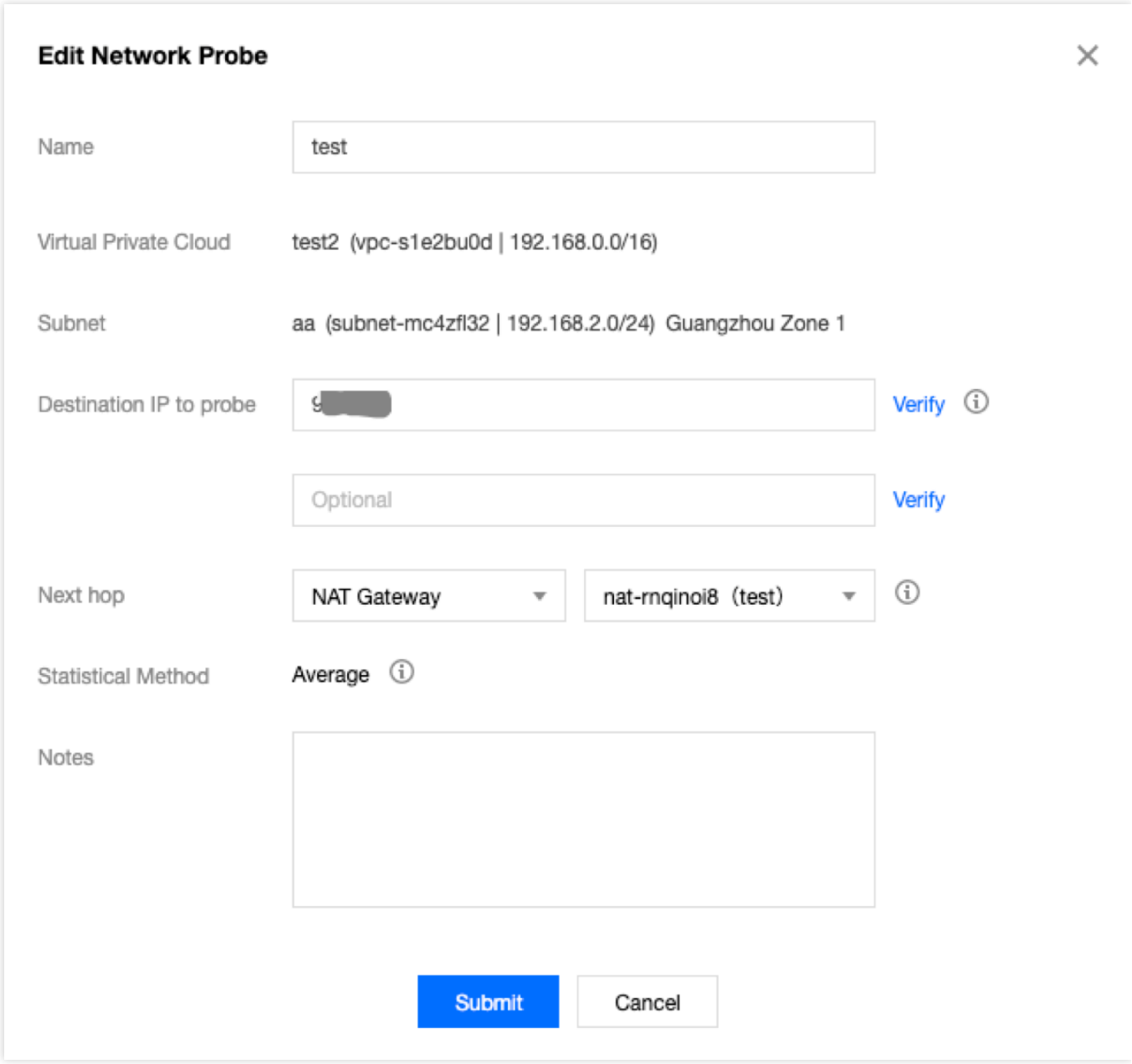
4. Di jendela pop-up **Edit Network Probe** (Edit Probe Jaringan), buat perubahan yang diperlukan dan klik **Submit** (Kirim) untuk menyimpan perubahan.

Keterangan:

Contoh ini belum menentukan hop selanjutnya.

Jika tidak ada hop selanjutnya yang ditentukan, nama, IP tujuan probe, dan catatan dari probe jaringan dapat dimodifikasi.

Jika hop selanjutnya ditentukan, nama, IP tujuan probe, sumber hop selanjutnya, dan catatan dari probe jaringan dapat dimodifikasi.

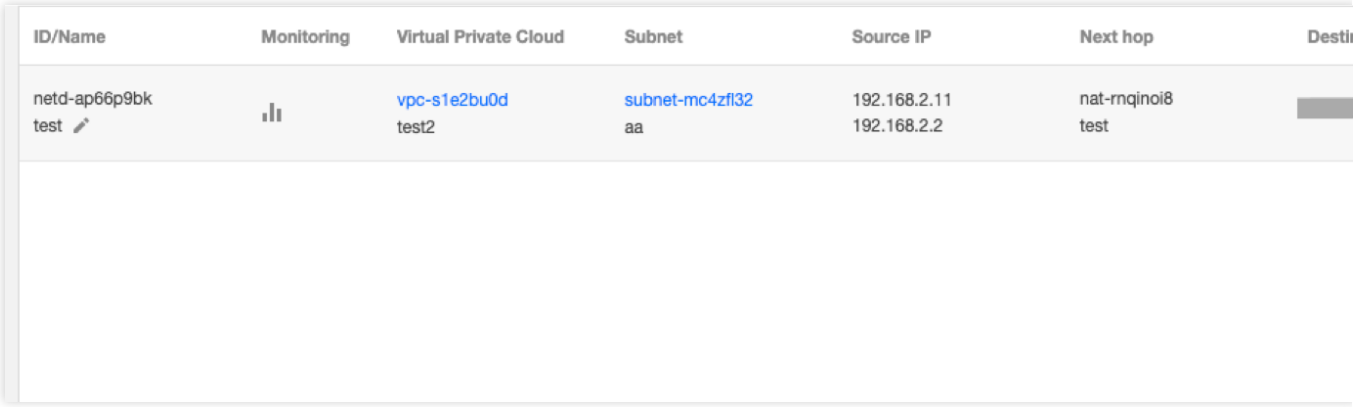


Menghapus Probe Jaringan

1. Login ke Konsol VPC.
2. Pilih **Diagnostic Tools** (Alat Diagnostik) -> **Network Probe** (Probe Jaringan) di bilah sisi kiri untuk masuk ke halaman pengelolaan.
3. Dalam daftar, temukan probe jaringan yang akan dihapus dan klik **Delete** (Hapus) di kolom operasi.
4. Klik **Delete** (Hapus) di jendela pop-up untuk mengonfirmasi penghapusan.

Perhatian:

Menghapus probe jaringan juga menghapus semua kebijakan yang peringatan yang terhubung dan rute yang dikonfigurasi. Periksa apakah bisnis Anda akan terpengaruh sebelum melanjutkan.



Mengonfigurasi Kebijakan Alarm

Anda dapat mengonfigurasi kebijakan alarm untuk layanan probe jaringan, sehingga Anda dapat segera mendeteksi pengecualian rute apa pun untuk membantu mengalihkan rute dengan cepat dan memastikan ketersediaan bisnis.

1. Login ke konsol CM dan buka halaman **Alarm Policy** (Kebijakan Alarm).
2. Klik **Create** (Buat).
3. Di jendela pop-up **Create Alarm Policy** (Buat Kebijakan Alarm), masukkan nama kebijakan, pilih **Network Probe** (Probe Jaringan) untuk jenis kebijakan, konfigurasikan objek alarm, kondisi pemicu alarm, dan kebijakan alarm, lalu klik **Complete** (Selesai).

Verifikasi Port Instans

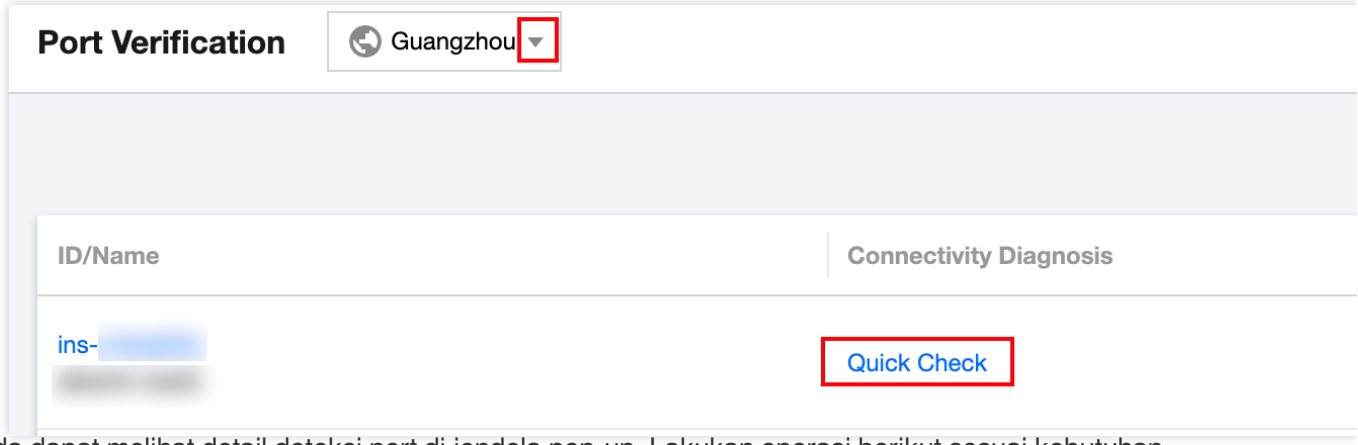
Waktu update terbaru：2024-01-24 17:55:51

Fitur verifikasi port instans dapat membantu Anda mendeteksi aksesibilitas port grup keamanan yang terkait dengan instans CVM, menemukan kesalahan, dan meningkatkan pengalaman pengguna.
Fitur ini mendukung deteksi aksesibilitas port umum dan port kustom. Lihat di bawah ini untuk port umum.

Aturan	Port	Deskripsi
Aturan masuk	Protokol ICMP	Digunakan untuk meneruskan pesan kontrol seperti perintah ping. ICMP adalah protokol kontrol, dan tidak ada port yang terlibat.
	TCP:20	Digunakan untuk mengizinkan unggah dan unduh melalui FTP.
	TCP:21	
	TCP:22	Digunakan untuk mengizinkan login SSH Linux.
	TCP:3389	Digunakan untuk mengizinkan login jarak jauh Windows.
	TCP:443	Digunakan untuk menyediakan layanan HTTPS situs web.
	TCP:80	Digunakan untuk menyediakan layanan HTTP situs web.
Aturan keluar	SEMUA	Digunakan untuk mengizinkan semua lalu lintas keluar untuk akses ke jaringan eksternal.

Panduan Operasi

1. Login ke Konsol VPC.
2. Klik **Diagnostic Tools** (Alat Diagnostik) > **Port Verification** (Verifikasi Port) di bilah sisi kiri untuk mengakses halaman pengelolaan.
3. Pilih wilayah di bagian atas halaman, temukan instans yang ingin Anda verifikasi dalam daftar, dan klik **Quick Check** (Periksa Cepat).



4. Anda dapat melihat detail deteksi port di jendela pop-up. Lakukan operasi berikut sesuai kebutuhan.

Hapus centang port yang tidak ingin Anda deteksi.

Masukkan port kustom untuk mendeteksi dan klik **Save** (Simpan).

Protokol: pilih TCP atau UDP.

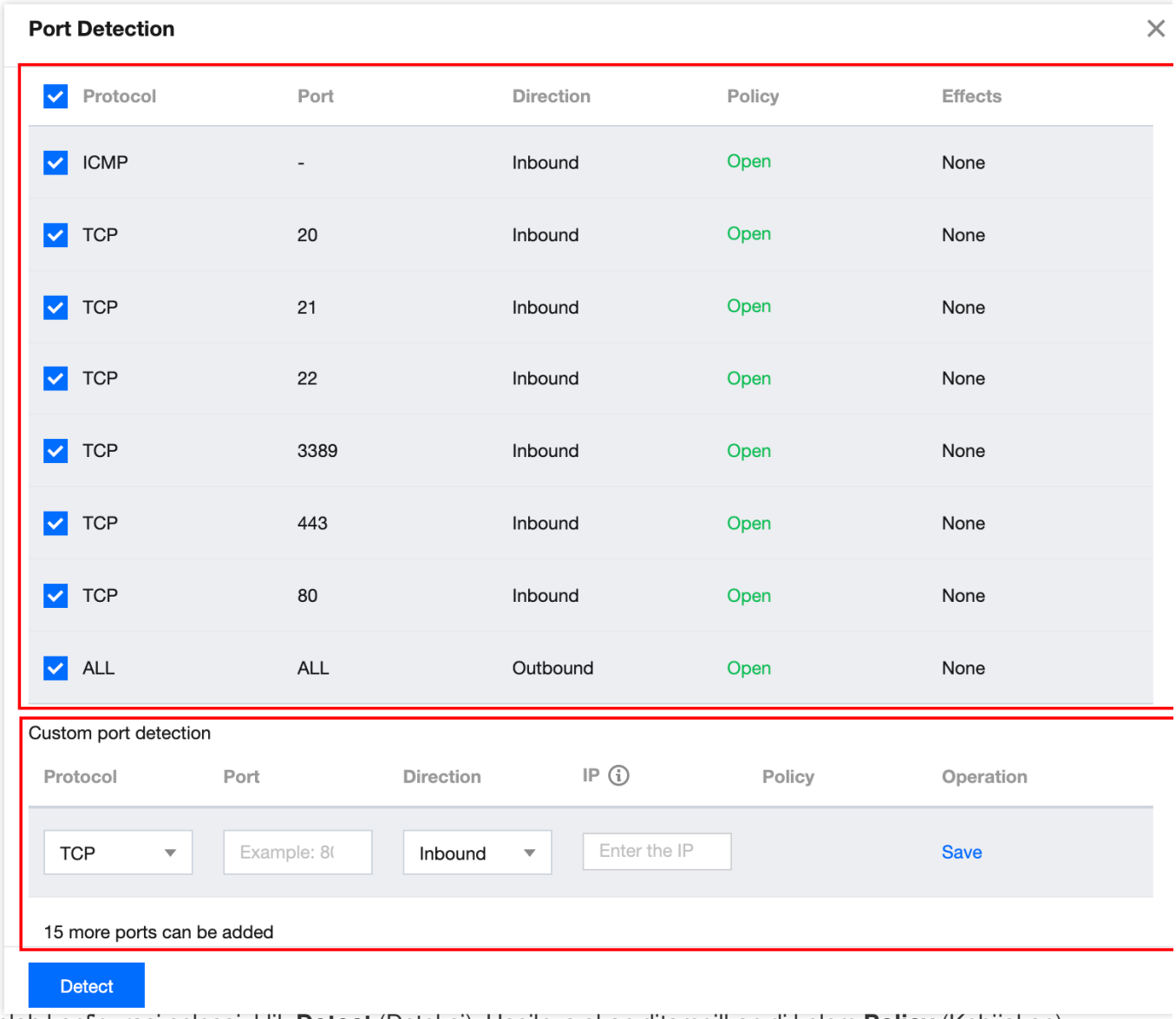
Port: masukkan satu nomor port untuk dideteksi, yang tidak boleh sama dengan port umum.

Arah: pilih **Inbound** (Masuk) atau **Outbound** (Keluar).

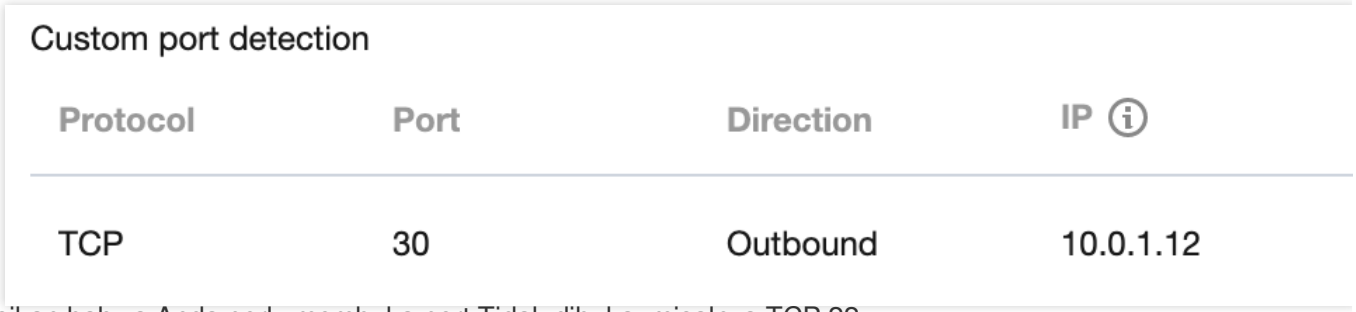
IP: masukkan IP sumber untuk arah masuk dan IP tujuan untuk arah keluar. Masukkan **ALL** (SEMUA) untuk semua alamat IP sumber dan tujuan.

Hingga 15 port kustom dapat dideteksi.

Jika Anda perlu mendeteksi lalu lintas keluar menuju IP 10.0.1.12 menggunakan protokol TCP melalui port 30, masukkan informasi berikut di area **Custom port detection** (Deteksi port kustom).



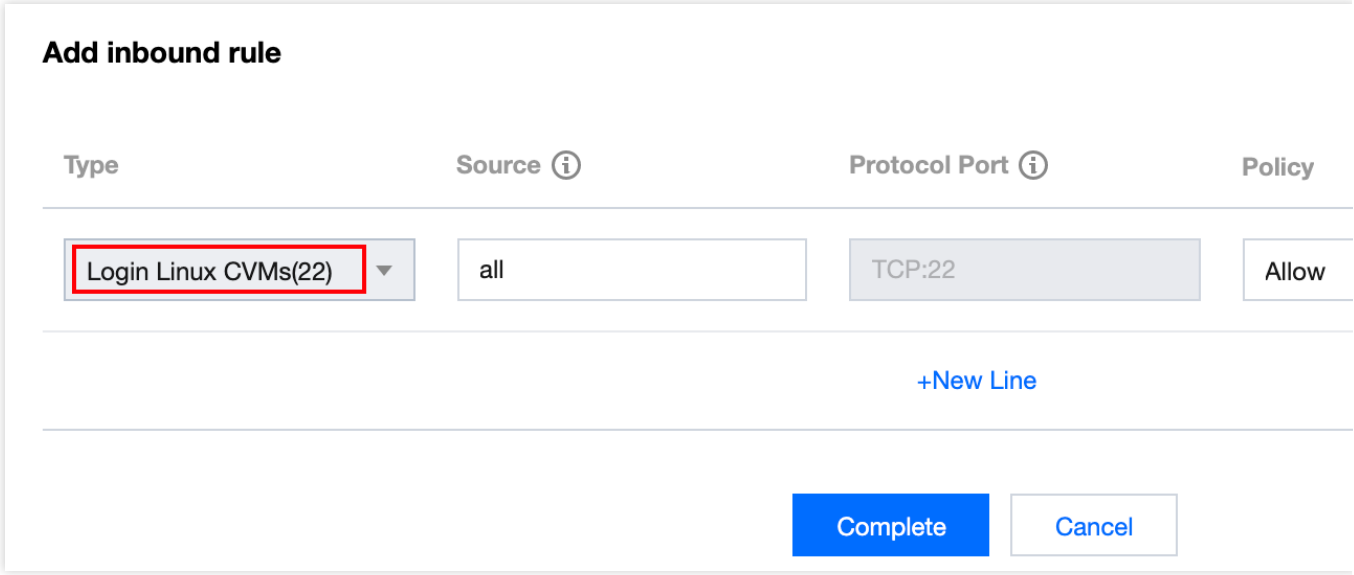
5. Setelah konfigurasi selesai, klik **Detect** (Deteksi). Hasilnya akan ditampilkan di kolom **Policy** (Kebijakan).



Asumsikan bahwa Anda perlu membuka port Tidak dibuka, misalnya TCP:22,

Kemudian Anda dapat menambahkan aturan masuk untuk grup keamanan yang terkait dengan instans di konsol Grup Keamanan untuk membuka port TCP:22. Anda dapat memilih semua untuk Sumber untuk mengizinkan semua

IP, atau memasukkan IP tertentu (rentang IP).



Informasi yang Relevan

Untuk informasi tentang grup keamanan, lihat Ikhtisar Grup Keamanan dan Menambahkan Aturan Grup Keamanan.
Untuk informasi selengkapnya tentang port umum, lihat Port Server Umum.

Flow Log

Waktu update terbaru：2024-01-24 17:55:51

Flow Logs (FL) menyediakan layanan penangkapan lalu lintas real-time, full-flow, dan non-intrusif sehingga Anda dapat menyimpan dan menganalisis lalu lintas jaringan secara real-time, membantu Anda melakukan pemecahan masalah, pengoptimalan arsitektur, pengujian keamanan, dan audit kepatuhan.

Operasi Umum

Membuat flow log
Membuat logset dan topik log
Menghapus flow log
Melihat entri flow log

Pencerminan Lalu Lintas

Ikhtisar

Waktu update terbaru：2024-01-24 17:55:51

Cermin lalu lintas menyediakan layanan pengumpulan lalu lintas yang memfilter dan menyalin lalu lintas yang diinginkan dari antarmuka jaringan yang ditentukan ke instans CVM di VPC yang sama. Fitur ini berlaku untuk kasus penggunaan termasuk audit keamanan, pemantauan risiko, pemecahan masalah, dan analisis bisnis.

Keterangan:

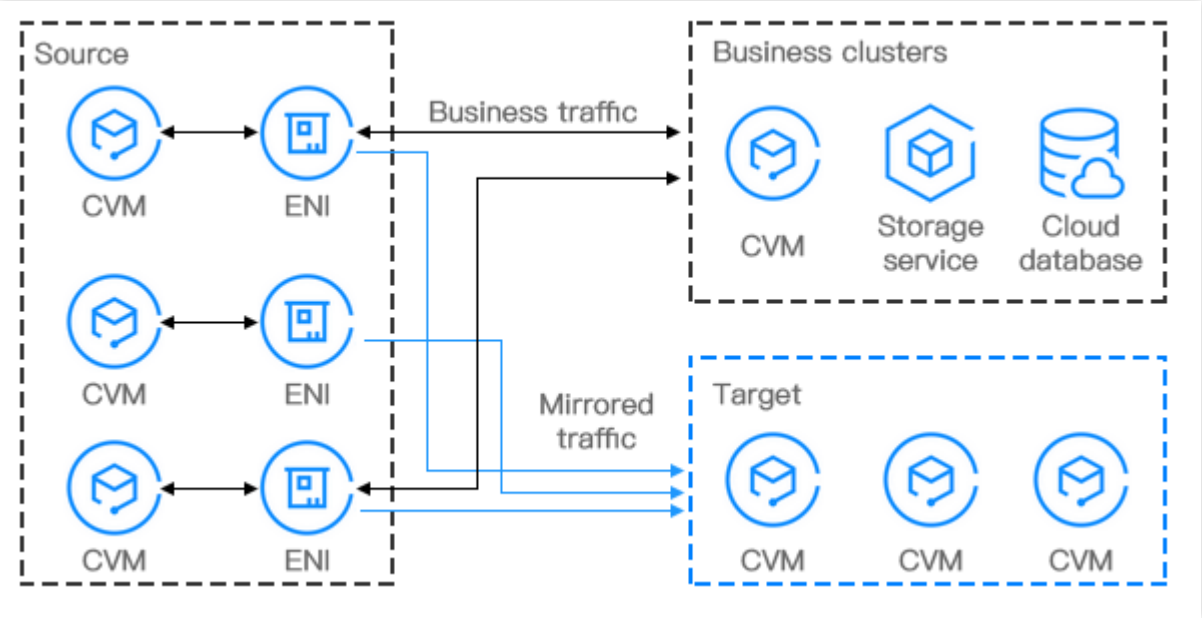
Namun, cermin lalu lintas menggunakan sumber informasi CVM seperti CPU, memori, dan bandwidth secara pro rata. Misalnya, jika Anda mencerminkan antarmuka jaringan yang memiliki lalu lintas masuk 1 Gbps dan lalu lintas keluar 1 Gbps. Dalam hal ini, instans perlu menangani 1 Gbps lalu lintas masuk dan 3 Gbps lalu lintas keluar (1 Gbps untuk lalu lintas keluar, 1 Gbps untuk lalu lintas masuk yang dicerminkan dan 1 Gbps untuk lalu lintas keluar yang dicerminkan).

Prosedur

Berikut ini adalah komponen kunci dari cermin lalu lintas, bersama dengan alur kerjanya.

Sumber: ENI yang ditentukan di VPC yang menerapkan aturan filter seperti jaringan, rentang koleksi, jenis koleksi, dan pemfilteran lalu lintas.

Target: IP penerima yang mendapatkan lalu lintas yang dikumpulkan.



Kasus Penggunaan

Audit keamanan

Sistem yang berjalan dapat menyebabkan lalu lintas jaringan yang tidak sehat atau menghasilkan pesan kesalahan karena pengecualian perangkat lunak, kesalahan perangkat keras, virus komputer, atau penggunaan yang tidak tepat. Untuk menemukan penyebab masalah ini, Anda dapat menggunakan cermin lalu lintas untuk menganalisis pesan jaringan.

Pemeriksaan intrusi

Untuk memastikan kerahasiaan, integritas, dan ketersediaan sumber daya sistem jaringan, Anda dapat menggunakan cermin lalu lintas untuk menyalin lalu lintas ke kluster CVM untuk analisis real-time.

Analisa bisnis

Gunakan cermin lalu lintas untuk menyajikan mode lalu lintas bisnis dengan jelas dan visual.

Batasan Layanan

Waktu update terbaru：2024-01-24 17:55:51

Pertimbangkan informasi berikut dan pertahankan bisnis Anda tetap utuh saat Anda menggunakan cermin lalu lintas.
Cermin lalu lintas saat ini dalam uji beta. Untuk menerapkannya, harap kirim tiket. Sebaiknya simpan tautan ke Konsol Cermin Lalu Lintas, sehingga Anda dapat login ke Konsol tanpa mendaftar lagi.
Cermin lalu lintas menggunakan sumber informasi CVM seperti CPU, memori, dan bandwidth secara pro rata.
Lalu lintas yang dicerminkan diperhitungkan terhadap bandwidth instans. Dampaknya tergantung volume dan jenis lalu lintas. Misalnya, jika Anda mencerminkan antarmuka jaringan yang memiliki lalu lintas masuk 1 Gbps dan lalu lintas keluar 1 Gbps. Dalam hal ini, instans perlu menangani 1 Gbps lalu lintas masuk dan 3 Gbps lalu lintas keluar (1 Gbps untuk lalu lintas keluar, 1 Gbps untuk lalu lintas masuk yang dicerminkan dan 1 Gbps untuk lalu lintas keluar yang dicerminkan).
Flow log tidak menangkap lalu lintas yang dicerminkan.
Batasan mengenai grup keamanan:
Sumber: lalu lintas yang dicerminkan tidak tunduk pada kebijakan grup keamanan.
Target: lalu lintas yang diterima tunduk pada kebijakan grup keamanan.
Cermin lalu lintas tidak tersedia untuk:
Protokol resolusi alamat
DHCP
Layanan metadata instans
NTP
Aktivasi Windows
Cermin lalu lintas mendukung pengumpulan lalu lintas dari ENI pada jenis CVM berikut:
Standar S1, Standar S2, Standar S3, Memori yang Dioptimalkan M1, Memori yang Dioptimalkan M2, Memori yang Dioptimalkan M3, IO Tinggi I1, IO Tinggi I2, IO Tinggi I3, Komputasi C2, Komputasi C3, CN3 yang dioptimalkan untuk Jaringan Komputasi, dan Big Data D1.

Membuat Cermin Lalu Lintas

Waktu update terbaru：2024-01-24 17:55:51

Cermin lalu lintas menyediakan layanan pengumpulan lalu lintas yang memungkinkan Anda memfilter lalu lintas dari ENI yang ditentukan menggunakan 5-tupel dan aturan lainnya. Kemudian Anda dapat menyalin lalu lintas yang difilter ke instans CVM di VPC yang sama. Fitur ini berlaku untuk kasus penggunaan termasuk audit keamanan, pemantauan risiko, pemecahan masalah, dan analisis bisnis. Dokumen ini menjelaskan cara membuat cermin lalu lintas.

Keterangan:

Fitur cermin lalu lintas saat ini dalam versi beta. Jika Anda ingin mencobanya, harap kirim tiket. Simpan tautan ke konsol Cermin Lalu Lintas untuk login nanti, jika tidak, Anda mungkin perlu mendaftar lagi.

Prasyarat

Pastikan IP sumber dan ENI target berada di VPC yang sama dan IP sumber memiliki tabel rute yang mengarah ke ENI target.

Petunjuk

Langkah 1: buat sumber cermin lalu lintas

1. Buka tautan yang Anda peroleh setelah mengirimkan tiket dan login ke konsol Cermin Lalu Lintas. Pada pemilih **Region** (Wilayah) atas, pilih wilayah tempat cermin lalu lintas akan dibuat.
2. Klik **+New** (+Baru).

Keterangan:

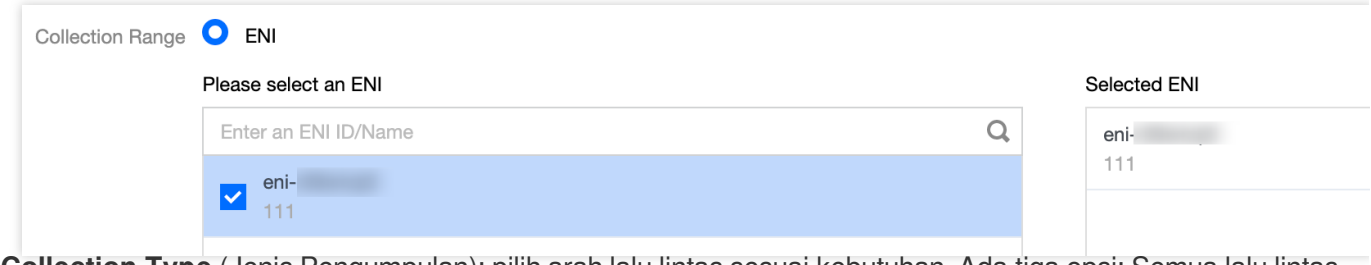
Hingga 5 cermin lalu lintas dapat dibuat dalam satu VPC.

3. Pada jendela pop-up, konfigurasikan sebagai berikut:

Masukkan nama untuk cermin lalu lintas (maksimal 60 karakter).

Pilih **Network** (Jaringan).

Pilih **ENI** (ENI) untuk **Collection Range** (Rentang Pengumpulan). - **ENI** (ENI): semua lalu lintas di VPC akan dikumpulkan, tetapi lalu lintas ENI yang terikat dengan IP penerima akan dikecualikan. Opsi ini memerlukan pemilihan ENI tertentu.

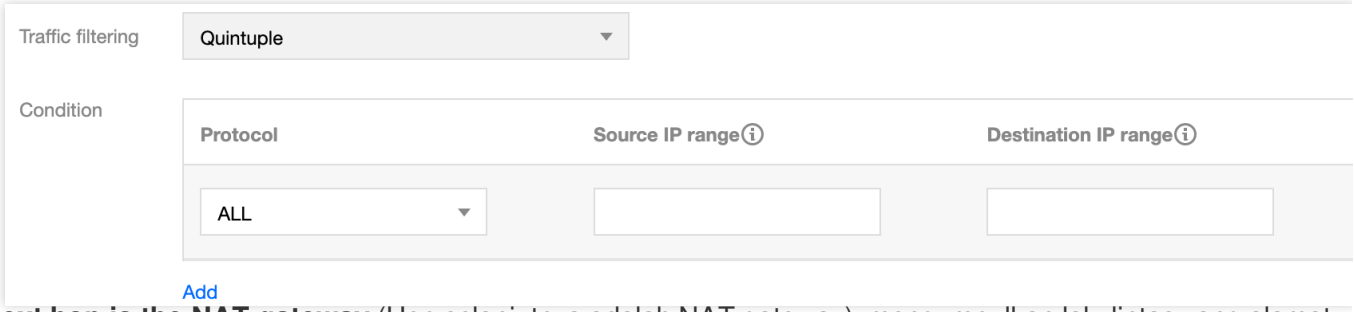


Pilih **Collection Type** (Jenis Pengumpulan): pilih arah lalu lintas sesuai kebutuhan. Ada tiga opsi: Semua lalu lintas, Lalu Lintas keluar dan Lalu Lintas masuk.

Pilih **Traffic filtering** (Pemfilteran lalu lintas): pilih metode untuk memfilter lalu lintas yang tidak diperlukan dan jaga agar cermin tetap berukuran kecil dan ringan.

N/A (T/A): semua lalu lintas yang dikonfigurasi akan dikumpulkan.

Quintuple (Quintuple): lalu lintas yang memenuhi ketentuan 5-tupel akan dikumpulkan. Setelah opsi ini dipilih, tentukan **Protocol** (Protokol), **Source IP range** (Rentang IP sumber), **Destination IP range** (Rentang IP tujuan), **Source port** (Port sumber), dan **Destination port** (Port tujuan). Anda dapat mengeklik **Add** (Tambahkan) untuk membuat kondisi filter lain. Hanya lalu lintas yang memenuhi semua ketentuan filter yang akan dikumpulkan.



The next hop is the NAT gateway (Hop selanjutnya adalah NAT gateway): mengumpulkan lalu lintas yang alamat hop selanjutnya adalah NAT gateway. Setelah opsi ini dipilih, pilih NAT gateway yang sesuai di sebelah **Condition** (Kondisi).

4. Setelah konfigurasi selesai, klik **Next** (Selanjutnya).

Langkah 2: buat target cermin lalu lintas

1. Atur lalu lintas penerima sebagai berikut:

Target type (Jenis target): pilih ENI target untuk menerima lalu lintas.

Keterangan:

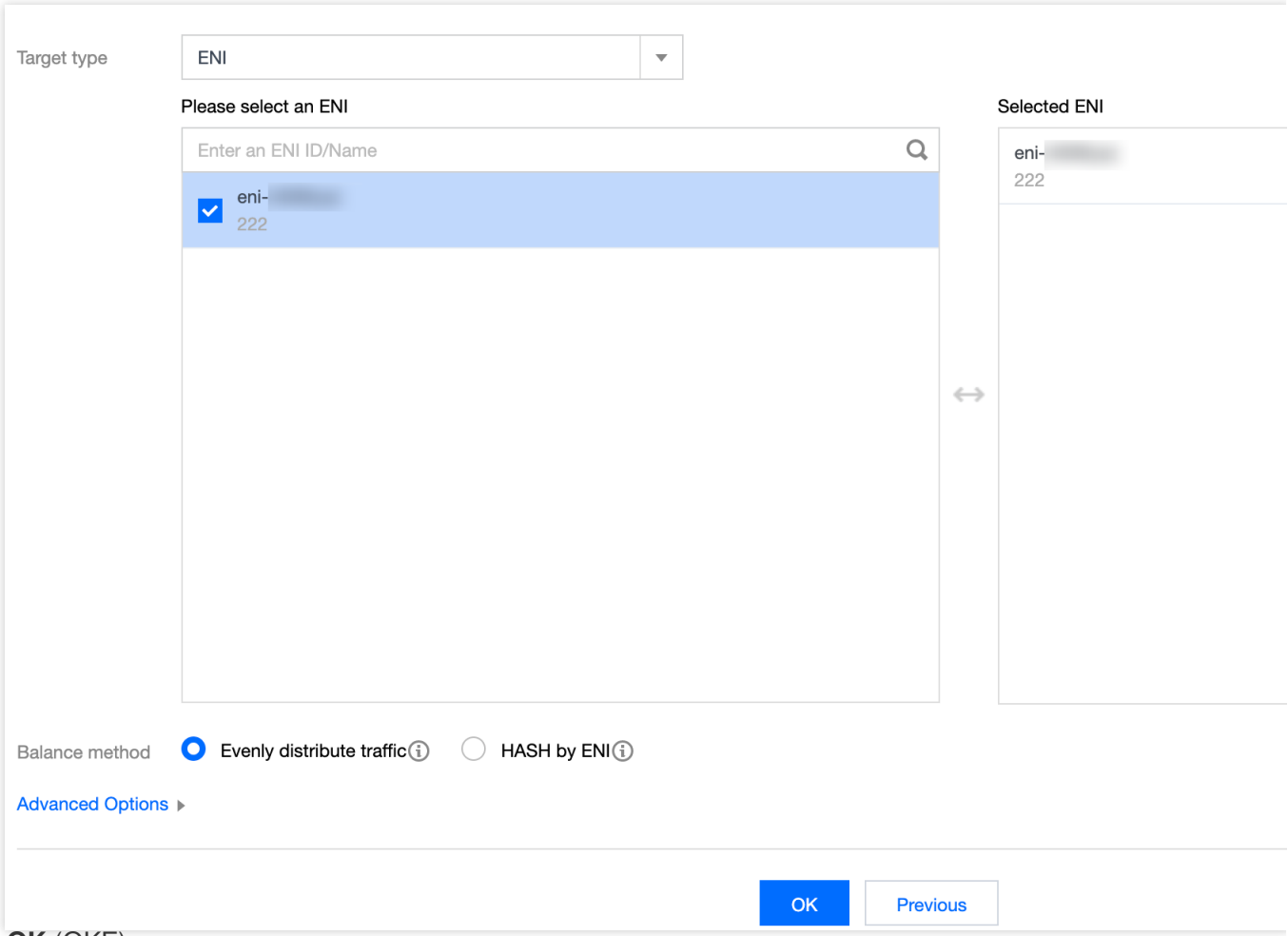
Setidaknya satu target ENI harus dipilih.

Lalu lintas ke ENI target dari dalam VPC tidak dikumpulkan.

Balance method (Metode Seimbang):

Evenly distribution (Distribusi merata): semua lalu lintas didistribusikan di antara semua ENI target secara merata.

HASH by ENI (HASH berdasarkan ENI): lalu lintas dari ENI selalu diteruskan ke ENI target tetap.



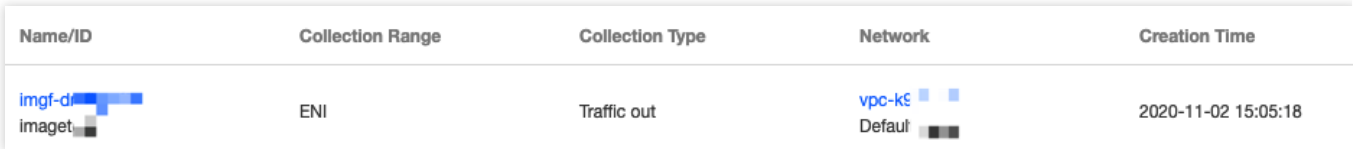
2. Klik **OK** (OKE).

Validasi Hasil

Perhatian:

Dokumen ini mengambil pembuatan cermin lalu lintas yang mengumpulkan lalu lintas keluar dari 10.0.0.14 ENI yang mengakses situs web www.qq.com sebagai contoh.

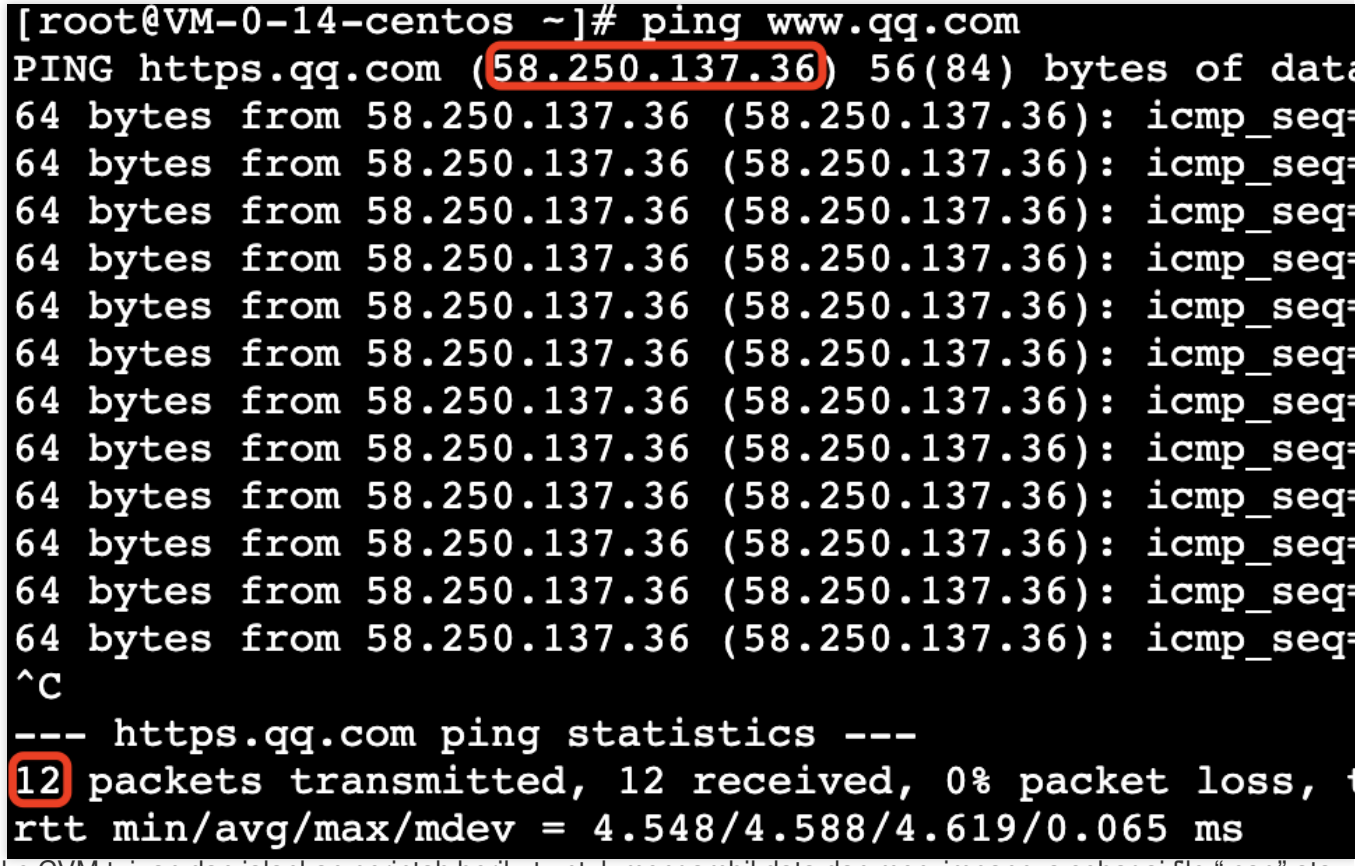
1. Kembali ke halaman **Traffic mirroring** (Pencerminan lalu lintas). Jika cermin lalu lintas yang baru saja Anda buat ditampilkan dengan **Collect Traffic** (Kumpulkan Lalu Lintas) diaktifkan, cermin lalu lintas telah berhasil dibuat.



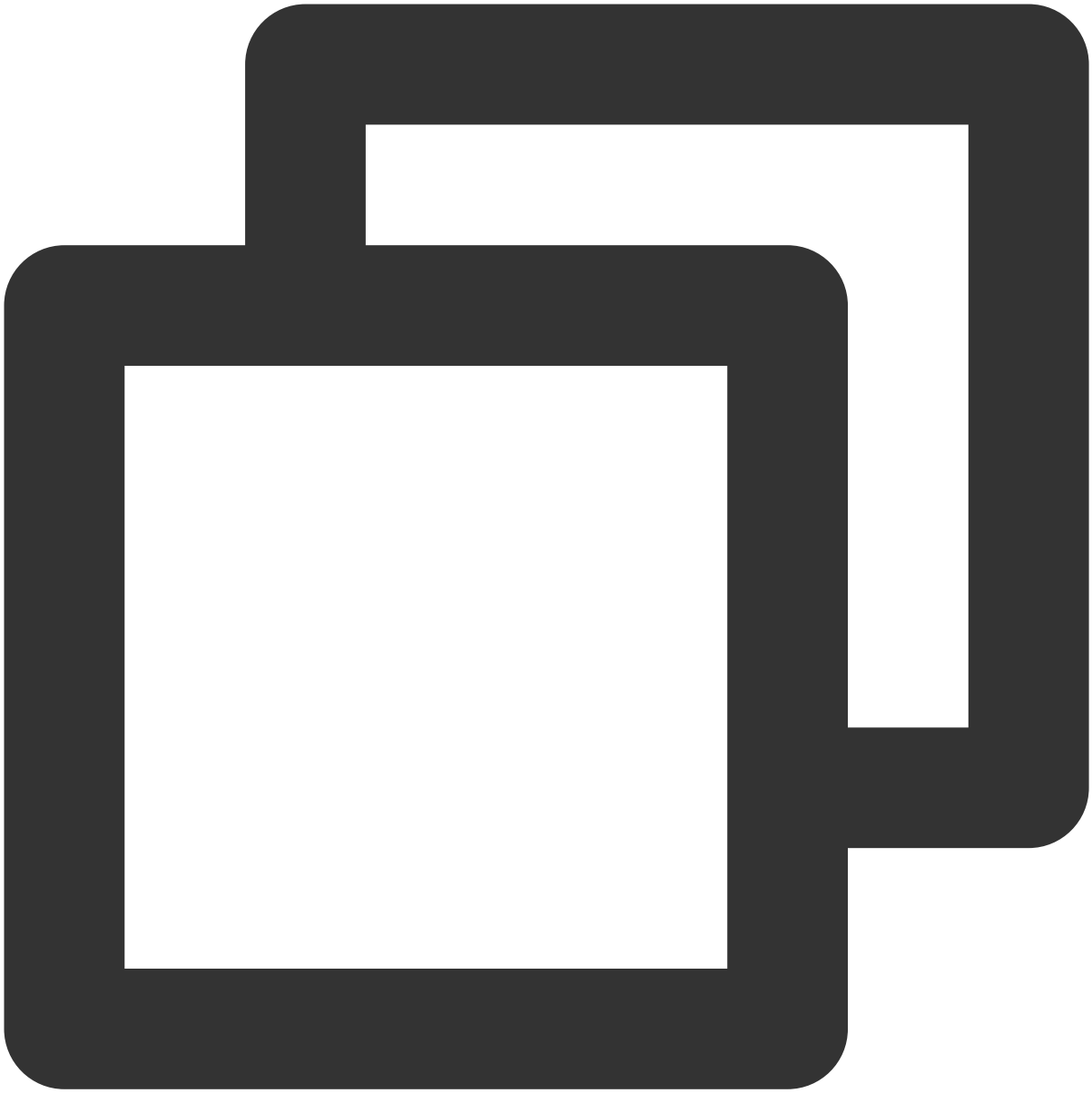
2. Lakukan langkah-langkah berikut untuk memverifikasi apakah lalu lintas yang dikumpulkan dicerminkan ke IP penerima.

2.1 Hasilkan lalu lintas ENI. Misalnya, Anda dapat login ke CVM sumber dan menjalankan perintah `ping public IP` (IP publik).

Source data: (Data sumber:)



Login ke CVM tujuan dan jalankan perintah berikut untuk mengambil data dan menyimpannya sebagai file “.cap” atau “.pcap”. Dokumen ini menggunakan file “.pcap” sebagai contoh.

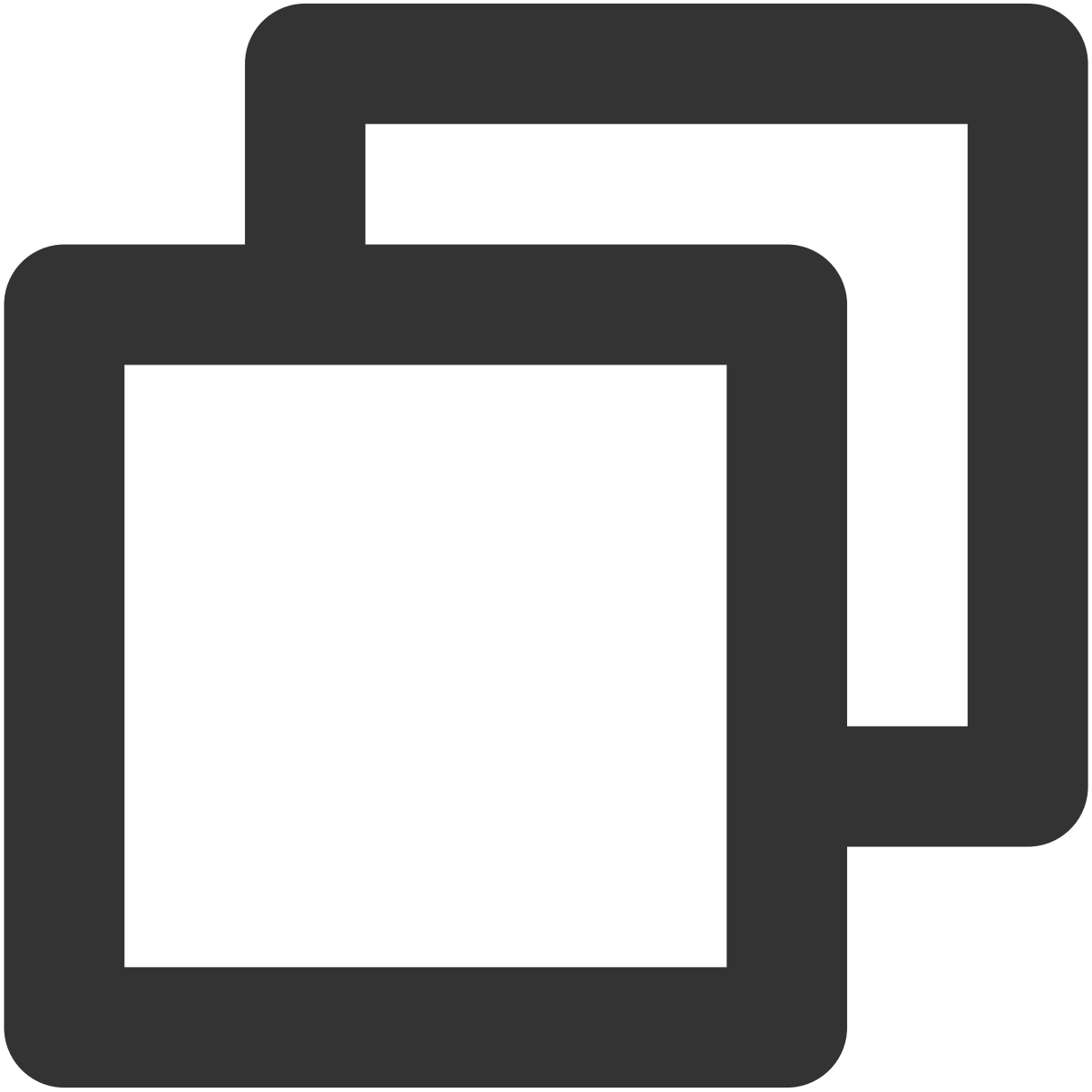


```
tcpdump -i eth0 -w capture-2020-10-27.pcap    #Masukkan nama file aktual.
```

Destination packets: (Paket tujuan:)

```
[root@VM-0-11-centos ~]# tcpdump -i eth0 -w capture-2020-10
tcpdump: listening on eth0, link-type EN10MB (Ethernet), ca
^C721 packets captured
735 packets received by filter
0 packets dropped by kernel
[root@VM-0-11-centos ~]# ls
capture-2020-10-27.pcap
```

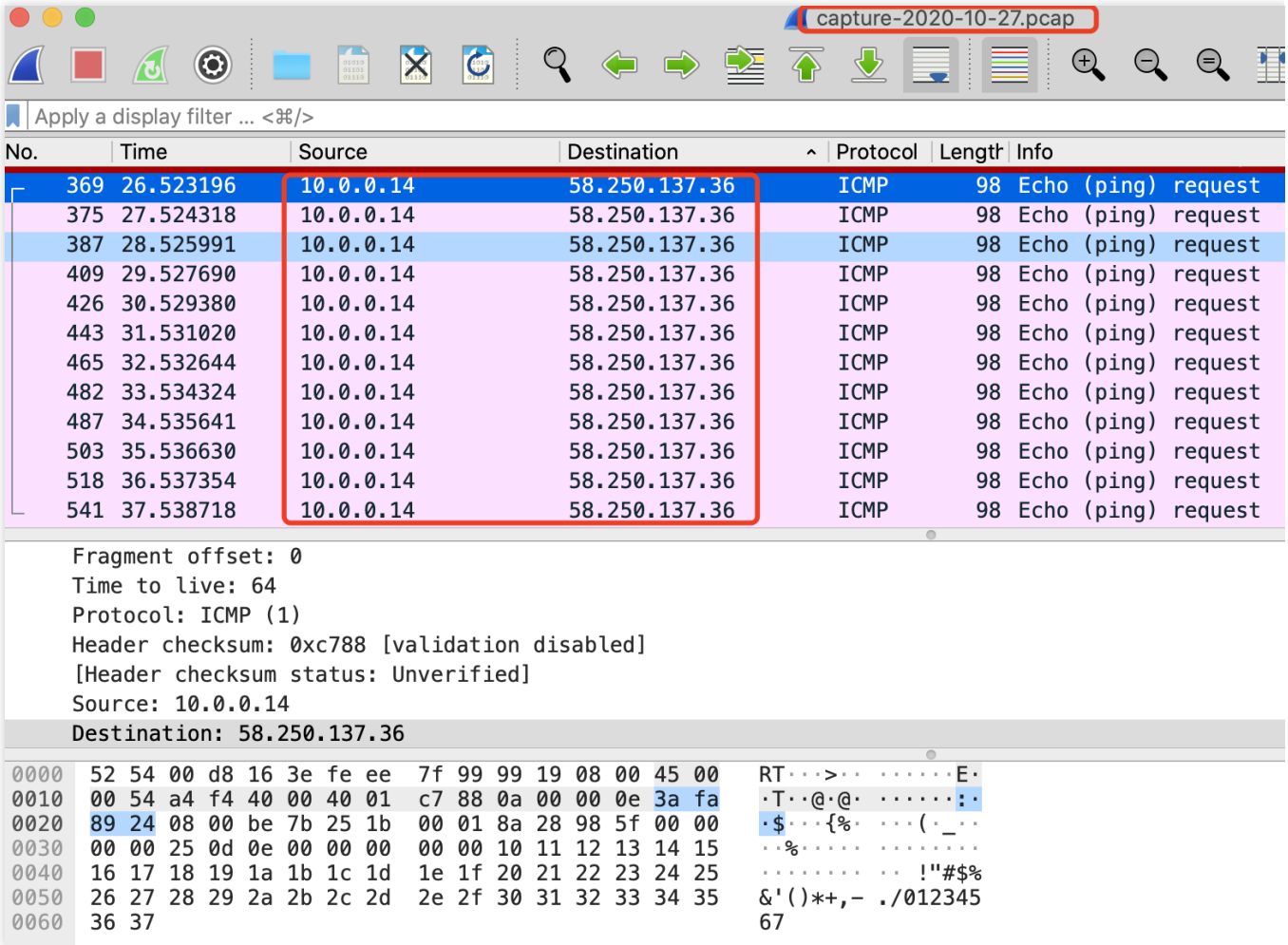
2.2 Gunakan simulator terminal (seperti SecureCRT) untuk login ke CVM tujuan dan mengekspor file yang disimpan di Langkah ii.



```
sz -bye capture-2020-10-27.pcap
```

2.3 Gunakan pengurai paket (seperti Wireshark) untuk mendapatkan data dari file “capture-2020-10-27.pcap” yang telah diunduh. Dalam contoh ini, 12 paket tercermin dari CVM sumber diperoleh dari CVM tujuan.

Packet verification: (Verifikasi paket:)



3. Jika paket luar biasa diperoleh, atau tidak dapat memperoleh paket, harap kirim tiket.

Operasi selanjutnya

Mengaktifkan atau menonaktifkan cermin lalu lintas

Memodifikasi cermin lalu lintas

Menambahkan tag

Menghapus cermin lalu lintas

Mengelola Cermin Lalu Lintas

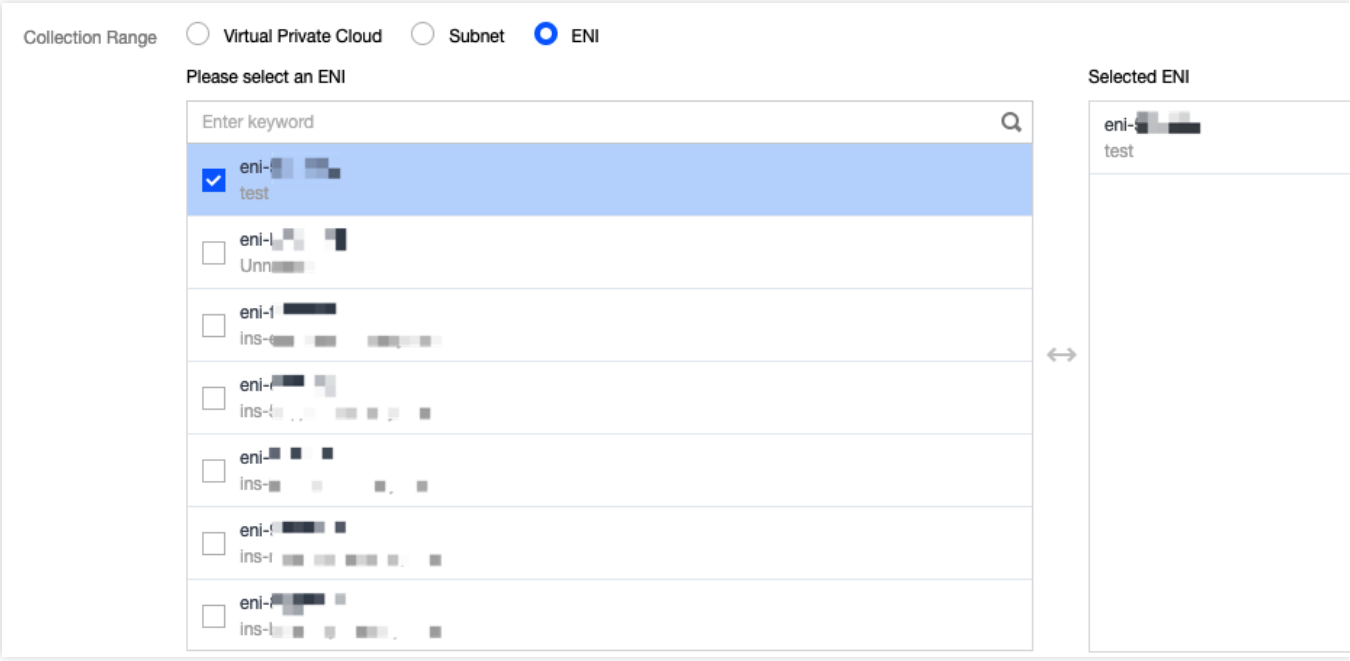
Waktu update terbaru：2024-01-24 17:55:51

Setelah cermin lalu lintas dibuat, Anda dapat mengaktifkan, menonaktifkan, mengubah atau menghapusnya, atau menambahkan tag d
i konsol.

Mengaktifkan atau Menonaktifkan Cermin Lalu Lintas

Tugas cermin lalu lintas baru diaktifkan secara default. Untuk menonaktifkannya dan mengaktifkannya kembali, ikuti langkah-langkah di bawah ini.

1. Buka tautan yang Anda peroleh setelah mengirimkan tiket dan login ke konsol Cermin Lalu Lintas. Pada pemilih **Region** (Wilayah) atas, pilih wilayah tempat cermin lalu lintas telah dibuat.
2. Temukan cermin lalu lintas yang ingin Anda kelola, nonaktifkan, atau aktifkan di bawah kolom **Collect Traffic** (Kumpulkan Lalu Lintas).



Memodifikasi Cermin Lalu Lintas

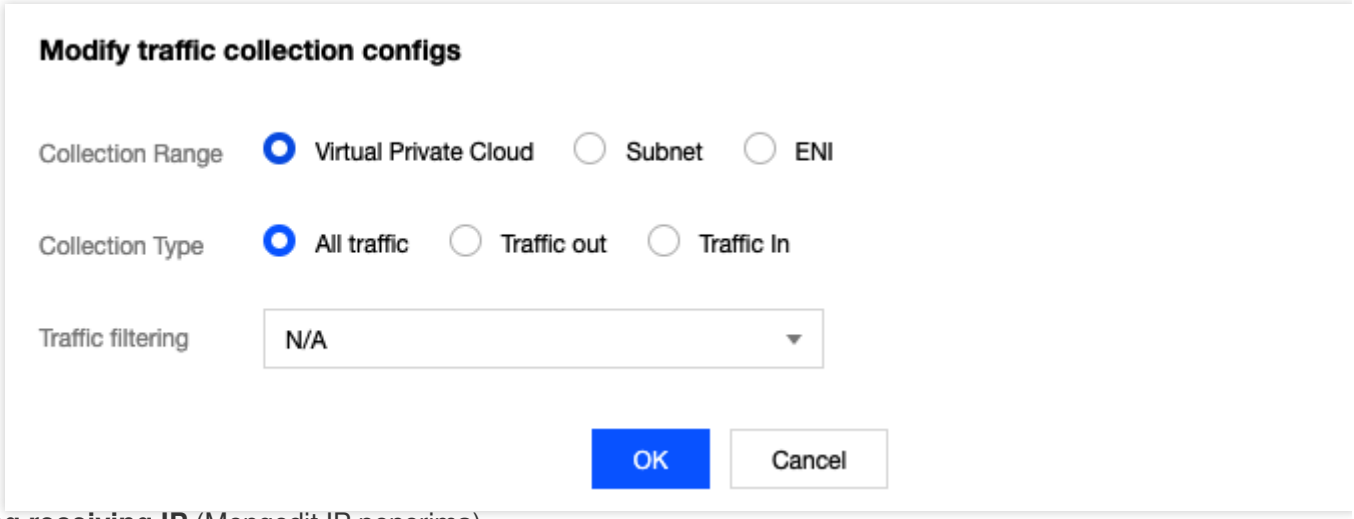
Untuk memo
difika
si cermin lalu lintas yang ada, ikuti langkah-langkah di bawah ini:

1. Buka tautan yang Anda peroleh setelah mengirimkan tiket dan login ke konsol Cermin Lalu Lintas. Pada pemilih **Region** (Wilayah) atas, pilih wilayah tempat cermin lalu lintas telah dibuat.
2. Pilih Nama/ID cermin lalu lintas yang akan dimodifikasi.
3. Ubah item yang diinginkan. Dokumen ini mengambil **Virtual Private Cloud** untuk **Collection Range** (Rentang Koleksi) sebagai contoh.

Editing traffic collecting configurations (Mengedit konfigurasi pengumpulan lalu lintas)

3.1.1 Klik **Edit** (Edit) di sudut kanan atas bagian Pengumpulan Lalu Lintas.

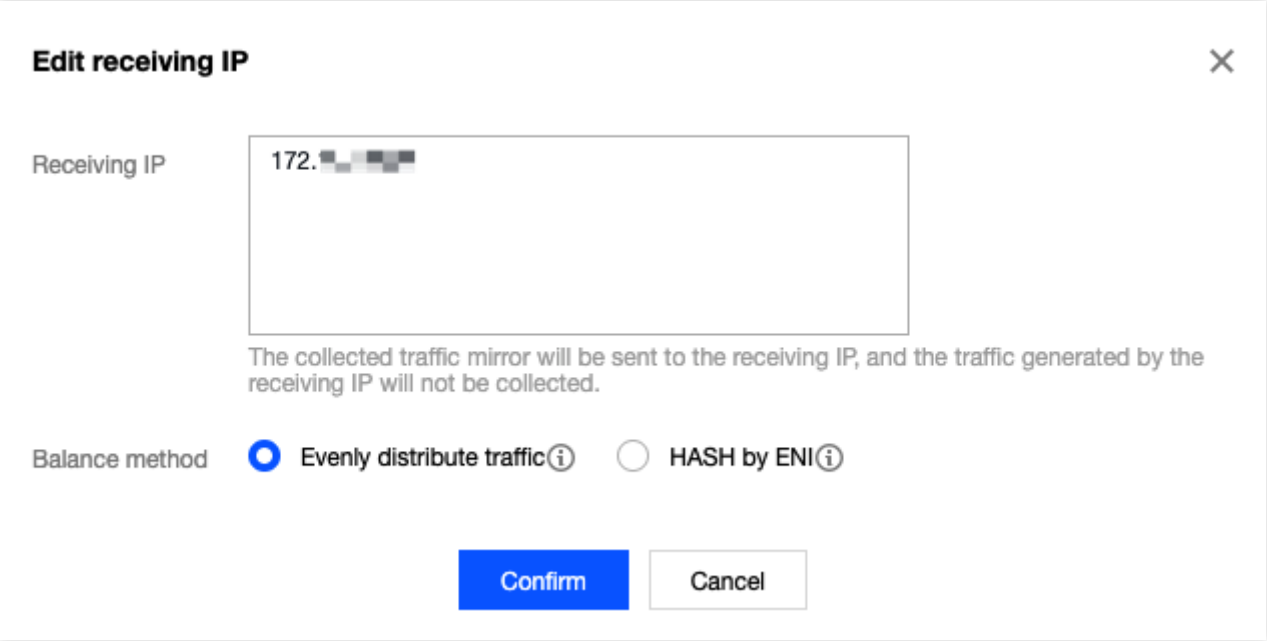
3.1.2 Pada jendela pop-up, ubah **Collection Range** (Rentang Koleksi), **Collection Type** (Jenis Koleksi), **Traffic filtering** (Pemfilteran lalu lintas), dan konfigurasi lainnya sesuai kebutuhan, lalu klik **OK** (Oke).



Editing receiving IP (Mengedit IP penerima)

3.1.1 Klik **Edit** (Edit) di sudut kanan atas bagian Menerima IP.

3.1.2 Pada jendela pop-up, ubah **Receiving IP** (Menerima IP) dan **Balance method** (Metode Saldo) sesuai kebutuhan, lalu klik **OK** (Oke).



Menambahkan Tag

Tag dig
unakan
untuk mengidentifikasi dan mengatur sumber informasi Tencent Cloud. Setiap tag berisi kunci tag dan nilai tag. Menambahkan tag ke cermin lalu lintas memudahkan untuk memfilter dan mengelola sumber informasi cermin lalu lintas.

1. Buka tautan yang Anda peroleh setelah mengirimkan tiket dan login ke konsol Cermin Lalu Lintas. Pada pemilih **Region** (Wilayah) atas, pilih wilayah tempat cermin lalu lintas telah dibuat.
2. Temukan cermin lalu lintas yang ingin Anda tambahkan tag, dan klik **Edit Tags** (Edit Tag) di bawah kolom **Operation** (Operasi).
3. Pada kotak dialog pop-up, konfigurasikan sebagai berikut:

3.1 Untuk **Tag key** (Kunci tag), masukkan nama kunci atau pilih dari daftar pilihan.

3.2 Untuk **Tag value** (Nilai tag), masukkan nilai kunci.

Keterangan:

Kunci tag mungkin tidak memiliki atau banyak nilai tag.

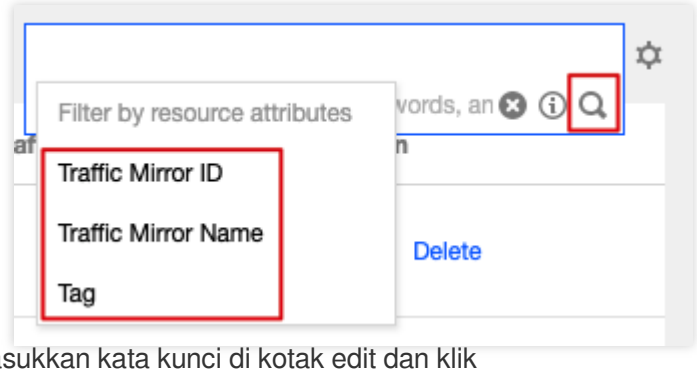
3.3 (Opsional) Klik **Add** (Tambahkan) dan konfigurasikan **Tag key** (Kunci tag) dan **Tag value** (Nilai tag) untuk menambahkan tag.

3.4 Setelah konfigurasi selesai, klik **OK** (Oke).

Menemukan Cermin Lalu Lintas

1. Klik

di kanan atas halaman **Traffic mirroring** (Pencerminan lalu lintas) dan pilih filter. Tiga filter seperti yang ditampilkan pada gambar berikut tersedia.



2. Masukkan kata kunci di kotak edit dan klik .

Keterangan:

Pisahkan kata kunci dengan bilah vertikal (|).

Menghapus Cermin Lalu Lintas

1. Buka tautan yang Anda peroleh setelah mengirimkan tiket dan login ke konsol Cermin Lalu Lintas. Pada pemilih **Region** (Wilayah) atas, pilih wilayah tempat cermin lalu lintas telah dibuat.
2. Temukan cermin lalu lintas yang akan dihapus, klik **Delete** (Hapus) di bawah kolom **Operation** (Operasi), dan konfirmasi penghapusan.

Peringatan Alarm dan Pemantauan

Waktu update terbaru：2024-01-24 17:48:51

Dengan mengonfigurasi kebijakan alarm, Anda dapat memantau status sumber daya pada VPC, seperti NAT gateway, VPN gateway, direct connect gateway, EIP, dll., untuk menemukan sumber daya cloud yang berjalan tidak normal dengan tepat waktu, menemukan dan memecahkan masalah SECEPAT MUNGKIN.

Mengonfigurasi Kebijakan Alarm

1. Login ke Konsol Cloud Monitor.
2. Pilih **Alarm Configuration** (Konfigurasi Alarm) > **Alarm Policy** (Kebijakan Alarm) di bilah sisi kiri untuk masuk ke halaman konfigurasi kebijakan alarm.
3. Klik **Create** (Buat), masukkan nama kebijakan, pilih sumber daya cloud VPC yang akan dikonfigurasi untuk jenis kebijakan, seperti **VPC** (VPC) > **EIP** (EIP), lalu konfigurasikan aturan alarm dan pemberitahuan alarm.
4. Klik **Complete** (Selesai). Anda dapat melihat kebijakan alarm yang diatur dalam daftar kebijakan alarm.

Keterangan:

Untuk menghapus kebijakan alarm, Anda harus melepas ikatan semua sumber daya terlebih dahulu.

5. Saat alarm dipicu, Anda akan menerima pemberitahuan alarm melalui saluran alarm yang dipilih (SMS/email/Pusat Pesan, dll.).

Konfigurasi kebijakan alarm untuk sumber daya cloud yang berbeda dijelaskan secara mendetail di bawah ini:
Direct Connect: Mengonfigurasi Kebijakan Alarm
NAT Gateway: - Mengatur Alarm
VPN Connection: Mengatur Alarm

Melihat Informasi Pemantauan

Anda dapat melihat informasi pemantauan sumber daya cloud yang sesuai di konsol VPC untuk membantu Anda memecahkan masalah kegagalan jaringan. Lihat:
Direct Connect: Melihat Data Pemantauan
CCN: Lihat Informasi Pemantauan
NAT Gateway: Melihat Informasi Pemantauan
Peering Connection: Melihat Data Pemantauan Lalu Lintas Jaringan Melalui Peering Connection Lintas Wilayah
VPN Connection: Melihat Data Pemantauan