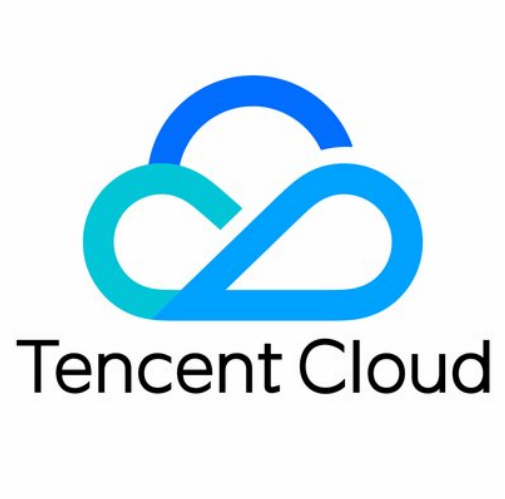
Virtual Private Cloud

Pertanyaan Umum

Dokumen produk



Direktori dokumen

Pertanyaan Umum
Umum
Konsep dan Fitur

Waktu update terbaru：2024-01-24 17:44:04

Bagaimana Anda membangun komunikasi antara subnet VPC yang berbeda?

Setiap VPC memiliki interkoneksi jaringan pribadi secara default, dan Anda dapat melihat rute default di tabel rute yang sesuai. Rute ini menunjukkan bahwa semua sumber daya di VPC ini dapat saling terhubung melalui jaringan pribadi.
Subnet di VPC yang berbeda tidak dapat terhubung melalui jaringan pribadi dan dapat saling berkomunikasi hanya dengan menggunakan Koneksi Peering atau CCN.

Dapatkah CVM yang berbeda di-deploy di zona ketersediaan yang berbeda di VPC yang sama?

Ya. VPC memiliki atribut wilayah (seperti Guangzhou, Beijing, atau Seoul), dan subnet di VPC memiliki atribut zona ketersediaan (seperti Zona 1 Guangzhou atau Zona 2 Guangzhou), sehingga subnet dalam VPC yang sama dapat digunakan di zona ketersediaan yang berbeda di wilayah yang sama. Atribut zona ketersediaan CVM mewarisi karakter subnetnya, dan CVM dibeli di bawah subnet di zona ketersediaan. Dengan demikian, CVM yang berbeda dapat digunakan di zona ketersediaan yang berbeda.

Bagaimana Anda membangun komunikasi antara CVM dan database di zona ketersediaan yang berbeda?

VPC yang sama: ada interkoneksi secara default. Jika tidak terhubung, Anda dapat memprioritaskan pemecahan masalah kebijakan firewall grup keamanan dan ACL jaringan .
VPC yang berbeda: Anda dapat menggunakan Peering Connection atau CCN untuk mengimplementasikan interkoneksi melalui jaringan pribadi antara dua VPC.

Berapa banyak alamat IP pribadi yang dapat diberikan setiap VPC untuk instans layanan Tencent Cloud?

Setiap VPC dapat menyediakan hingga 65.533 alamat IP pribadi untuk instans layanan Tencent Cloud.

Apa itu CIDR?

Classless Inter-Domain Routing (CIDR) mengimplementasikan pembagian jaringan secara keseluruhan menggunakan blok alamat ruang jaringan independen yang Anda tentukan bersama dengan IP dan mask. Ini menghilangkan konsep tradisional rentang dan subnetting tradisional kelas A, kelas B, dan kelas C serta

mengalokasikan ruang alamat IP lebih efektif. Saat membuat VPC dan subnet, Anda perlu membuat rentang IP yang sesuai dalam bentuk blok CIDR. Misalnya, untuk membuat rentang IP `10.0.16.0 – 10.0.17.255`, maka: Konversi `10.0.16.0 – 10.0.17.255` ke format biner `00001010.00000000.0001000.000000000 – 00001010.00000000.00010001.11111111`, dengan 23 bit pertama harus sama. Format blok CIDR setelah konversi adalah `10.0.16.0/23`.

Mengapa saya tidak dapat menghapus VPC dan subnet setelah secara manual menghentikan instans TencentDB for Redis?

Jika hanya ada satu instans TencentDB for Redis di VPC, setelah instans dihentikan secara manual, instans tersebut akan dipindahkan ke keranjang sampah TencentDB. Saat ini, sumber daya Redis belum benar-benar dilepas, sehingga VPC tidak dapat segera dihapus. Anda dapat mengatasi masalah ini dengan cara berikut:
Di keranjang sampah TencentDB, **eliminate** (hilangkan) instans TencentDB for Redis, lalu hapus VPC dan subnet.
Tunggu hingga instans TencentDB for Redis kedaluwarsa secara otomatis di keranjang sampah TencentDB, lalu hapus VPC dan subnet.
Untuk informasi selengkapnya, lihat Menghentikan Instans.

Mengapa aplikasi untuk EIP gagal?

Jika kuota EIP terlampaui, aplikasi EIP akan gagal. Untuk informasi selengkapnya tentang cara melihat detail kuota, harap lihat Batas kuota EIP.

IP dan Rentang IP

Waktu update terbaru：2024-01-24 17:44:04

Berapa batasan rentang IP VPC dan subnet?

Blok CIDR Tencent Cloud VPC mendukung penggunaan salah satu dari rentang IP pribadi berikut:
`10.0.0.0` - `10.255.255.255` (rentang mask antara 12 hingga 28)
`172.16.0.0` - `172.31.255.255` (rentang mask antara 12 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.

Dapatkah rentang IP VPC dan subnet diubah?

Saat membuat VPC dan subnet, Anda perlu menentukan blok CIDR-nya, dan blok tersebut tidak dapat diubah setelah dibuat.
Jika Anda tidak dapat membuat koneksi peering karena tumpang tindihnya rentang IP VPC, Anda dapat mencoba Cloud Connect Network, yang memiliki detail batas yang lebih kecil (hanya rentang IP subnet yang tidak dapat tumpang tindih) atau memigrasikan instans ke VPC lain. Untuk detailnya, lihat Beralih dari Jaringan Klasik ke VPC.

Apa yang harus dilakukan ketika koneksi peering gagal dibuat karena konflik rentang IP VPC?

Saat membuat koneksi peering, blok CIDR dari dua VPC tidak boleh tumpang tindih, atau akan menyebabkan koneksi peering gagal dibuat.
Jika rentang IP subnet dari dua VPC yang perlu berkomunikasi tidak tumpang tindih, maka Anda dapat menggunakan CCN untuk membangun komunikasi. CCN menurunkan batas rentang IP ke tingkat subnet saat VPC berkomunikasi. Misalnya, jika rentang IP dari dua VPC yang perlu saling berkomunikasi adalah `10.0.0.0/16`, tetapi subnetnya masing-masing adalah `10.0.1.0/24` dan `10.0.2.0/24`, maka Anda dapat membangun komunikasi menggunakan CCN. Lihat Dokumentasi Produk CCN.
Jika kebutuhan Anda tidak terpenuhi dengan menggunakan CCN, maka Anda perlu memigrasikan sumber daya di dalam subnet yang tumpang tindih tersebut.
Untuk detail tentang mengubah subnet CVM, lihat Mengubah Subnet Instans.
Migrasikan instans dalam VPC seperti yang diinstruksikan di Beralih ke VPC.

Dapatkah saya mengubah IP pribadi sumber daya di VPC (CVM dan database)?

Anda dapat mengubah IP pribadi utama dari ENI utama CVM, tetapi IP pribadi utama ENI sekunder tidak dapat diubah. Untuk detailnya, lihat Memodifikasi Alamat IP Pribadi.
Anda dapat memodifikasi IP pribadi instans TencentDB (seperti instans MySQL). Lihat Menyesuaikan IP dan Port.
IP pribadi CLB tidak dapat diubah.

Dapatkah saya memigrasikan CVM atau database dari satu VPC ke VPC lainnya?

Untuk saat ini, Anda dapat memigrasikan instans CVM dan instans TencentDB for MySQL ke VPC lain di bawah akun yang sama. Instans TencentDB lainnya tidak didukung.
Lihat Beralih ke VPC untuk memigrasikan instans dalam jaringan dasar ke VPC.
Untuk memigrasikan TencentDB untuk instans MySQL, lihat Beralih Jaringan.

Apa yang dilakukan oleh EIP?

EIP berlaku untuk skenario berikut:
1. **Disaster recovery** (Pemulihan bencana)
Kami sangat menyarankan Anda menggunakan EIP untuk pemulihan bencana. Ketika salah satu CVM Anda gagal menyediakan layanan secara normal, Anda dapat melepaskan ikatan EIP dari CVM ini dan mengikatnya kembali ke CVM yang sehat untuk melanjutkan layanan dengan cepat.
2. **Retaining a specific public IP** (Mempertahankan IP publik tertentu)
Jika perlu mempertahankan IP publik tertentu pada akun Anda, Anda bisa mengubahnya menjadi EIP, yang selanjutnya bisa digunakan untuk mengakses jaringan publik setelah diikat dengan perangkat. EIP ini akan dipertahankan pada akun Anda sampai Anda "melepasnya"
3. **Other special scenarios** (Skenario khusus lainnya)
Saat Anda perlu mengubah IP dalam kasus khusus lainnya, Anda dapat mengonversi IP publik biasa menjadi EIP, kemudian mengikat/melepas ikatan EIP. Namun, dengan sumber daya EIP terbatas yang tersedia, kuota dikenakan pada jumlah EIP untuk setiap wilayah dalam satu akun. Oleh karena itu, perencanaan yang wajar dan penggunaan EIP sangat penting.

Bagaimana cara menjaga agar IP publik tidak berubah?

Jika perlu mempertahankan IP publik tertentu pada akun Anda, Anda bisa mengubahnya menjadi EIP, yang selanjutnya bisa digunakan untuk mengakses jaringan publik setelah diikat dengan perangkat. EIP ini akan dipertahankan pada akun Anda sampai Anda "melepasnya"
Untuk petunjuk, lihat Mengonversi UP publik umum ke EIP.

Apakah EIP bisa dikonversi kembali menjadi IP publik?

EIP tidak bisa dikonversi kembali ke IP publik.

Jaringan Klasik Terkait

Waktu update terbaru：2024-01-24 17:44:04

Apa perbedaan antara jaringan klasik dan VPC?

VPC adalah ruang jaringan virtual yang terisolasi secara logis di Tencent Cloud.
VPC menyediakan lebih banyak fitur daripada jaringan klasik. Untuk informasi tentang cara mengoperasikan Classiclink, lihat Mengelola Jaringan Klasik.

Dapatkah saya mengalihkan CVM dari jaringan klasik ke VPC?

Ya. Tencent Cloud memungkinkan Anda memigrasikan satu atau beberapa instans CVM dari jaringan klasik ke VPC sekaligus. Untuk langkah dan petunjuk selengkapnya, lihat Beralih ke VPC.

Perhatian:

Operasi ini tidak dapat dibatalkan. Pastikan Anda membaca dokumen dengan cermat sebelum melakukan operasi ini.

Dapatkah saya mengalihkan CVM dari VPC ke jaringan klasik?

Tidak. VPC mendukung lebih banyak fitur dengan fleksibilitas yang lebih besar, oleh karena itu kami menyarankan Anda untuk memigrasikan CVM dari jaringan klasik ke VPC.

Bagaimana cara membangun komunikasi antara CVM jaringan klasik dan CVM berbasis VPC?

Anda dapat menggunakan Classiclink untuk menjalin komunikasi antara jaringan klasik dan VPC.
Penggunaan Classiclink tunduk pada batasan berikut:
1. Jaringan klasik dan VPC yang akan dikomunikasikan terletak di wilayah yang sama (dapat berada di zona ketersediaan yang berbeda, seperti Zona 1 Guangzhou dan Zona 2 Guangzhou).
2. Rentang alamat IP VPC (CIDR) harus 10.0.0.0/16 - 10.0.47.0/16 (termasuk subset). Jika tidak, akan ada konflik.
Jika jaringan klasik dan VPC Anda memenuhi ketentuan ini, Anda dapat mengonfigurasi Classiclink pada halaman detail VPC di konsol, untuk mengaitkan VPC dengan CVM jaringan klasik untuk interkoneksi.

Dapatkah sumber daya seperti penyeimbang beban cloud dan database di jaringan klasik berkomunikasi dengan VPC?

Koneksi terminal membantu membangun komunikasi antara instans di VPC dan instans lain di jaringan klasik melalui jaringan pribadi. Ini memetakan alamat IP instans jaringan klasik ke IP VPC, yang memungkinkan Anda mengakses instans jaringan klasik melalui IP VPC. Produk jaringan klasik termasuk CLB klasik, TencentDB, CMEM, REDIS, dan MongoDB dapat berkomunikasi dengan VPC dengan cara ini. Komunikasi lintas wilayah atau lintas akun tidak didukung.
Arah: Satu arah (VPC mengakses jaringan klasik).
Jika diperlukan, kirim tiket untuk menerapkan.

Dapatkah jaringan klasik dan instans VPC di bawah akun yang berbeda saling berkomunikasi?

Tidak. VPC mendukung lebih banyak fitur dengan fleksibilitas yang lebih besar, oleh karena itu kami sarankan Anda untuk memigrasikan sumber daya dari jaringan klasik ke VPC.

Bagaimana cara membatalkan pengaitan CVM dari VPC atau jaringan klasik?

Lakukan langkah-langkah berikut untuk membatalkan pengaitan CVM.

1. Login ke Konsol VPC.
2. Klik ID VPC yang saling terhubung dengan jaringan klasik untuk masuk ke halaman detail VPC.
3. Klik **Classiclink** (Classiclink). Dalam daftar CVM jaringan klasik, pilih CVM yang akan dibatalkan pengaitannya dan klik **Disassociate** (Batalkan Pengaitan).
4. Klik **OK** (Oke).

Untuk petunjuk langkah demi langkah, lihat bagian “Membatalkan pengaitan VPC dan CVM Jaringan Klasik” di Mengelola Jaringan Klasik.

Tentang Kuota Produk

Waktu update terbaru：2024-01-24 17:44:04

Apakah ada batas kuota untuk instans VPC? Berapa banyak VPC yang dapat dibuat untuk setiap akun?

Beberapa sumber daya VPC tunduk pada batas kuota penggunaan. Secara default, satu akun dapat membuat hingga 20 VPC di setiap wilayah.

Berapa banyak EIP yang dapat diterapkan oleh satu akun?

Setiap akun Tencent Cloud dapat diterapkan hingga 20 EIP di setiap wilayah.
Untuk setiap akun Tencent Cloud, batas atas harian peluang pembelian default hingga 40 (kuota * 2). Setelah EIP tidak terikat, setiap akun dapat dialihkan dengan alamat IP publik 10 kali per hari secara gratis.
Setiap akun tagihan per CVM memiliki kuota harian gratis 10 kesempatan untuk mendapatkan alamat IP publik setelah melepas ikatan EIP. Untuk informasi selengkapnya, lihat bagian **Quota Limits** (Batas Kuota) di IP Elastis (EIP).

Koneksi

Koneksi ke Jaringan Publik

Waktu update terbaru：2024-01-24 17:44:04

Bagaimana cara menerapkan IP publik jika tidak ditetapkan pada saat membeli CVM?

Jika IP publik tidak ditetapkan saat Anda membeli CVM, maka tidak ada cara untuk menerapkan ulang IP publik biasa untuk CVM ini. Namun, fungsi yang sama dapat dilakukan menggunakan EIP. Untuk informasi selengkapnya tentang cara menggunakannya, lihat Menerapkan untuk EIP.

EIP adalah jenis IP publik yang ditetapkan ke alamat IP publik tertentu di wilayah tertentu. Tidak seperti IP publik biasa, EIP terikat ke akun Anda. Dengan kata lain, Anda dapat mengikat dan melepaskan ikatan EIP dengan CVM yang berbeda sesuai kebutuhan (hanya satu yang dapat diikat dalam sekali waktu).

Karena sifat khusus dari EIP, jika Anda menerapkan EIP tetapi tidak mengikatnya ke instans, biaya sumber daya IP akan dikenakan. Untuk detail selengkapnya, lihat Penagihan EIP.

Bagaimana sebuah instans (CVM atau database) dapat mengakses jaringan publik tanpa alamat IP publik?

Instans tanpa IP publik dapat diterapkan untuk EIP (lihat pertanyaan sebelumnya) atau dapat mengakses jaringan publik melalui gateway NAT.

Gateway NAT dapat menyediakan fitur SNAT dan DNAT untuk instans CVM di VPC. Jika Anda memiliki beberapa instans dan ingin instans tersebut mengakses jaringan publik melalui IP publik yang sama, Anda dapat menggunakan gateway NAT.

Anda bisa mengubah IP publik CVM.

Ya.

Jika instans CVM Anda menggunakan IP publik yang ditetapkan pada saat pembelian, silakan lihat Mengubah Alamat IP Publik.

Jika instans CVM Anda terikat ke EIP, Anda harus melepas ikatan EIP terlebih dahulu, lalu menerapkan untuk EIP lain atau mengikat EIP yang ada.

Perhatian:

Sebaiknya segera lepaskan EIP setelah dikonversi dari IP publik. Jika tidak, EIP yang tidak terikat dengan instans akan dikenakan biaya sumber daya IP.

Apakah IP publik yang sebelumnya digunakan dapat dipulihkan? Apakah EIP tertentu dapat diterapkan?

Anda dapat memulihkan IP publik yang sebelumnya Anda gunakan dan saat ini tidak ditetapkan ke pengguna lain. IP publik yang dipulihkan semuanya adalah EIP. Untuk informasi selengkapnya, lihat Mendapatkan alamat IP jaringan publik.

Apakah penambahan kuota dapat dilakukan setelah jumlah EIP mencapai batas atas?

Karena sumber daya EIP terbatas, Anda hanya dapat menerapkan 20 akun per akun per wilayah, dan Anda tidak dapat meminta peningkatan kuota. Instans CVM tanpa IP publik dapat menggunakan gateway NAT dan metode lain untuk mengakses jaringan publik.

Bagaimana cara CVM mengakses jaringan publik jika memiliki IP publik atau EIP dan subnetnya juga dikaitkan dengan gateway NAT?

Jika CVM memiliki IP atau EIP publik dan subnetnya juga dikaitkan dengan gateway NAT (artinya tabel rute menentukan bahwa hop selanjutnya untuk lalu lintas subnet ini untuk mengakses jaringan publik adalah gateway NAT), maka pengaturan default adalah untuk semua lalu lintas CVM ini guna mengakses jaringan publik melalui gateway NAT.
Jika Anda perlu mengubah prioritas agar lalu lintas dari instans CVM ke jaringan publik melewati IP publik, lihat Menyesuaikan Prioritas Gateway NAT dan EIP.

Ketika instans CVM mengakses jaringan publik melalui gateway publik atau gateway NAT, apakah biaya jaringan akan dikenakan dua kali?

Tidak, biaya jaringan hanya akan dikenakan satu kali. Saat mengakses jaringan publik melalui gateway publik atau gateway NAT, hanya biaya jaringan gateway publik yang sesuai atau biaya jaringan gateway NAT yang akan dikenakan.

Komunikasi Inter-VPC

Waktu update terbaru：2024-01-24 17:44:04

Bagaimana CVM atau Database Berinterkoneksi melalui Jaringan Pribadi?

Komunikasi jaringan pribadi CVM atau database di VPC sebenarnya adalah komunikasi alamat IP pribadi di tingkat jaringan, dan oleh karena itu tidak ada perbedaan di antara keduanya. Metode komunikasi di bawah skenario alamat IP pribadi yang berbeda adalah sebagai berikut:

Skenario Komunikasi	Metode Komunikasi
Wilayah berbeda	CVM atau database di wilayah berbeda dimiliki oleh instans VPC yang berbeda dan saling berkomunikasi melalui peering connection atau CCN. (Baik komunikasi akun yang sama maupun lintas akun didukung.)
Zona ketersediaan berbeda	VPC yang sama: mendukung interkoneksi secara default. Instans VPC yang berbeda: berkomunikasi melalui koneksi peering atau CCN. (Baik komunikasi akun yang sama maupun lintas akun didukung.)
Instans VPC yang berbeda	Berkomunikasi melalui koneksi peering atau CCN. (Baik komunikasi akun yang sama maupun lintas akun didukung.)
Subnet yang berbeda	VPC yang sama: mendukung interkoneksi secara default. VPC yang berbeda: berkomunikasi melalui koneksi peering atau CCN. (Baik komunikasi akun yang sama maupun lintas akun didukung.)
Lintas akun	Komunikasi lintas-akun melalui koneksi peering atau CCN. (Baik komunikasi wilayah yang sama dan lintas wilayah didukung.)

Perhatian:

Untuk interkoneksi VPC lintas akun melalui koneksi peering atau CCN, perhatikan hal-hal berikut:

Akun root memiliki sumber daya. Jika Anda ingin berkomunikasi dengan akun lain melalui koneksi peering atau CCN, masukkan akun root.

Sub-akun hanya memiliki izin operasi secara default. Terapkan izin dari akun root untuk membuat koneksi peering atau CCN jika diperlukan.

Private network default interconnection (Interkoneksi default jaringan pribadi) ada di antara subnet yang berbeda dengan VPC yang sama (baik berada di zona ketersediaan yang sama maupun tidak). Jika tidak dapat saling terhubung, Anda dapat memecahkan masalah kebijakan firewall grup keamanan dan ACL jaringan terlebih dahulu.

Apa yang Harus Saya Lakukan Ketika Koneksi Peering Gagal Dibuat Karena Konflik Rentang IP VPC?

Saat Anda mencoba membuat koneksi peering, blok CIDR dari dua instans VPC tidak boleh tumpang tindih, jika tidak, koneksi peering tidak dapat dibuat.
Jika rentang IP dari kedua instans VPC yang perlu saling berkomunikasi tumpang tindih tetapi rentang IP subnet tidak tumpang tindih, maka Anda dapat mencoba membangun komunikasi melalui CCN. CCN dapat menurunkan batas rentang alamat IP ke tingkat subnet saat instans VPC saling berkomunikasi.
Misalnya, rentang IP dari kedua instans VPC yang perlu saling berkomunikasi adalah `10.0.0.0/16`, tetapi subnetnya masing-masing adalah `10.0.1.0/24` dan `10.0.2.0/24`. Dalam kasus ini, Anda dapat membangun komunikasi melalui CCN. Untuk informasi selengkapnya, lihat CCN.
Jika kebutuhan Anda tidak dapat dipenuhi menggunakan CCN, Anda perlu memigrasikan sumber daya di dalam subnet yang tumpang tindih.
Untuk detail tentang mengubah subnet CVM, lihat Mengubah Subnet Instans.
Untuk detail tentang migrasi antar-VPC, lihat Mengalihkan Instans VPC.

Jika VPC1 Secara Terpisah Membuat Koneksi Peering Dengan VPC2 dan VPC3, Lalu Bisakah VPC2 dan VPC3 Saling Berkomunikasi?

Tidak, tidak bisa. Dua instans VPC dapat membuat interkoneksi melalui koneksi peering, tetapi hubungan interkoneksi ini tidak transitif. Ini berarti bahwa ketika koneksi peering dibuat antara VPC1 dan VPC2, sementara koneksi peering lain dibuat antara VPC1 dan VPC3, interkoneksi lalu lintas tidak tersedia antara VPC2 dan VPC3 karena koneksi peering tidak transitif.

Classiclink-Terkait

Waktu update terbaru：2024-01-24 17:44:05

Apa itu Classiclink?

Classiclink digunakan untuk mengaitkan CVM di jaringan klasik ke VPC tertentu, yang memungkinkan CVM berkomunikasi dengan layanan Tencent Cloud, termasuk CVM dan database di VPC. Untuk informasi selengkapnya, lihat Mengelola Jaringan Klasik.

Bagaimana cara membangun komunikasi antara CVM di jaringan klasik dan CVM di VPC?

Anda dapat menggunakan Classiclink untuk membangun komunikasi antara jaringan klasik dan VPC.
Saat menggunakan Classiclink, perhatikan batasan berikut:
1. Jaringan klasik dan VPC yang perlu saling berkomunikasi harus berada di wilayah yang sama (tetapi dapat berada di zona ketersediaan yang berbeda, seperti Zona 1 Guangzhou dan Zona 2 Guangzhou).
2. CIDR (rentang IP) VPC harus `10.0.0.0/16 – 10.47.0.0/16` (termasuk subset), jika tidak, konflik akan terjadi.
3.
Jika jaringan klasik dan VPC Anda memenuhi ketentuan ini, Anda dapat mengonfigurasi tab **Classiclink** (Classiclink) pada halaman detail VPC di Konsol untuk mengaitkan VPC dengan CVM di jaringan klasik untuk interkoneksi.

Dapatkah sumber daya, termasuk penyeimbang beban awan dan database di jaringan klasik, berkomunikasi dengan VPC?

Koneksi terminal membantu membangun komunikasi antara instans di VPC dan instans lain di jaringan klasik melalui jaringan pribadi. Prinsipnya adalah memetakan alamat IP instans di jaringan klasik ke alamat IP VPC, sehingga Anda dapat mengakses instans jaringan klasik dengan mengakses alamat IP VPC yang sesuai. Layanan yang mendukung jaringan klasik termasuk CLB klasik, TencentDB, CMEM, REDIS, MongoDB. Namun, komunikasi lintas wilayah atau lintas akun tidak didukung.
Arah: satu arah (VPC mengakses jaringan klasik).
Jika Anda memerlukan petunjuk selengkapnya, kirim tiket untuk menerapkan.

Apakah instans jaringan dan VPC klasik yang berada di akun yang berbeda dapat saling berkomunikasi?

Tidak. Saat ini, sumber daya (CVM dan database) di jaringan klasik dan instans VPC di bawah akun yang berbeda tidak dapat saling berkomunikasi. VPC mendukung lebih banyak fitur dengan fleksibilitas yang lebih besar, jadi sebaiknya Anda memigrasi dari jaringan klasik ke VPC.

Keamanan

Keamanan VPC-Terkait

Waktu update terbaru：2024-01-24 17:44:05

Bagaimana Cara Memastikan Keamanan CVM di Instans VPC?

VPC sendiri adalah lingkungan jaringan yang terisolasi secara logis, dan lalu lintas dapat dikontrol dengan mengonfigurasi grup keamanan dan ACL jaringan:
Grup keamanan: menyediakan kontrol lalu lintas jaringan untuk CVM di tingkat instans. Lalu lintas yang tidak diizinkan untuk masuk atau keluar dari instans secara otomatis ditolak.
ACL Jaringan: menyediakan kontrol lalu lintas jaringan tingkat subnet.

Port dan Grup Keamanan

Waktu update terbaru：2024-01-24 17:44:04

Pertanyaan umum terkait port

Port mana yang harus dibuka ke Internet sebelum saya login ke instans?

Biasanya, Anda perlu membuka port 22 untuk instans Linux, atau port 3389 untuk instans Windows. Untuk informasi selengkapnya, lihat Kasus Aplikasi Grup Keamanan.

Mengapa saya harus membuka port, dan bagaimana caranya?

Anda harus membuka port di grup keamanan untuk menggunakan layanan terkait.
Misalnya, jika Anda ingin mengakses halaman web menggunakan port 8080, Anda harus membuka port ini di grup keamanan.
Langkah-langkah untuk membuka port:
1. Masuk ke Konsol Grup Keamanan, dan klik ID/nama grup keamanan yang terikat dengan instans ini untuk masuk ke halaman detailnya.
2. Pilih **Inbound/Outbound rule** (Aturan Masuk/Keluar) dan klik **Add a Rule** (Tambahkan Aturan).
3. Masukkan alamat IP (rentang) dan port yang akan dibuka, lalu pilih **Allow** (Izinkan) untuk membuka port.
Untuk informasi selengkapnya, lihat Menambahkan Aturan Grup Keamanan.

Bisnis saya tidak dapat diakses setelah saya mengubah port.

Setelah mengubah port layanan, Anda juga perlu membuka port yang sesuai dalam grup keamanan.

Port mana yang tidak didukung oleh Tencent Cloud?

Port berikut tidak diizinkan karena memiliki risiko keamanan dan kemungkinan besar akan diblokir oleh ISP.

Protokol	Port yang tidak didukung
TCP	42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900 dan 9996
UDP	1026, 1027, 1434, 1068, 5554, 9996, 1028, 1433 dan 135 - 139

Saya tidak dapat terhubung ke alamat eksternal melalui port TCP 25.

Untuk meningkatkan kualitas pengiriman email melalui alamat IP Tencent Cloud, CVM diblokir agar tidak menggunakan port TCP 25 untuk terhubung ke alamat eksternal secara default. Untuk membuka blokir port ini, Anda dapat login ke konsol, arahkan kursor ke area navigasi akun di bagian atas, dan klik **Security Control** (Kontrol Keamanan) guna melihat tautan untuk membuka blokir port 25.
Setiap akun mendukung pembukaan blokiran CVM sebanyak 5 kali. Perhatikan bahwa CVM bayar sesuai pemakaian tidak didukung.

Untuk informasi selengkapnya, lihat Port Server Umum.

Pertanyaan Umum terkait Grup Keamanan

Mengapa ada aturan penolakan yang ditetapkan secara default di grup keamanan?

Aturan grup keamanan dipilih untuk berlaku berdasarkan urutannya dari atas ke bawah, jadi setelah aturan izinkan yang pertama kali ditetapkan divalidasi, maka aturan lainnya akan ditolak secara default. Jika aturan membuka semua port ke Internet, maka aturan penolakan akhir akan menjadi tidak valid. Kami menyediakan pengaturan default ini karena masalah keamanan.

Jika saya mengikat grup keamanan yang salah dengan sebuah instans, apa pengaruhnya terhadap instans tersebut? Bagaimana memperbaikinya?

Potential problems (Potensi masalah)
Anda mungkin gagal terhubung dalam jarak jauh ke instans Linux melalui SSH atau instans Windows melalui desktop jarak jauh.
Anda mungkin gagal melakukan ping ke IP publik dan alamat IP pribadi dari instans CVM dalam jarak jauh di grup keamanan ini.
Anda mungkin gagal mengakses melalui HTTP layanan web yang diekspos oleh instans CVM dalam grup keamanan ini.
Anda mungkin gagal mengakses Internet dengan instans di bawah grup keamanan ini.
Solutions (Solusi)
Jika salah satu masalah di atas terjadi, Anda dapat membuka "Security Group Management" (Manajemen Grup Keamanan) di konsol dan mengatur ulang aturan untuk grup keamanan, misalnya ke "only bind all-pass security groups by default" (hanya mengikat grup keamanan all-pass secara default).
Untuk detail pengaturan aturan grup keamanan, lihat Grup Keamanan - Aturan Grup Keamanan.

Apa yang dimaksud dengan arah dan kebijakan grup keamanan?

Kebijakan grup keamanan bekerja dalam arah keluar dan masuk. Yang pertama adalah untuk memfilter lalu lintas keluar dari CVM, dan yang terakhir adalah untuk memfilter lalu lintas masuk dari CVM.
Kebijakan grup keamanan dibagi menjadi lalu lintas **allow** (izinkan) dan **refuse** (tolak).

Bagaimana urutan penerapan kebijakan grup keamanan?

Urutan penerapan kebijakan grup keamanan adalah dari atas ke bawah. Lalu lintas melewati urutan pencocokan grup keamanan dari atas ke bawah, dan kebijakan tersebut berlaku segera setelah ada kecocokan yang berhasil.

Mengapa port yang dibuka ke Internet oleh grup keamanan tidak dapat mengakses instans CVM?

CVM terikat dengan beberapa grup keamanan, dan port ini ditolak oleh grup keamanan lain dengan prioritas lebih tinggi.
ACL jaringan atau firewall telah dikonfigurasi.

Mengapa IP yang tidak diizinkan oleh grup keamanan masih dapat mengakses CVM?

Kemungkinan alasan:
CVM terikat ke beberapa grup keamanan, dan IP ini diizinkan oleh grup keamanan lain.
Alamat IP ini milik layanan publik Tencent Cloud yang disetujui.

Bisakah iptable digunakan bersama dengan grup keamanan?

Ya, iptable dan grup keamanan dapat digunakan secara bersamaan. Lalu lintas Anda akan difilter dua kali sebagai berikut:
Keluar: proses dalam instans Anda > iptable > grup keamanan.
Masuk: grup keamanan > iptable > proses di instans Anda.

Semua CVM yang dikaitkan dengan grup keamanan telah ditampilkan. Namun, saya masih tidak bisa menghapus grup keamanan.

Selain CVM, grup keamanan juga dapat diikat dengan instans database CLB, ENI dan cloud. Harap pastikan bahwa semua instans yang terikat dengan grup keamanan yang akan dihapus telah dibatalkan pengaitannya.

Bisakah nama grup keamanan kloning sama dengan nama grup keamanan di wilayah target?

Ya.

Dapatkah saya mengkloning grup keamanan ke proyek atau wilayah lain menggunakan API?

Ya. Untuk informasi selengkapnya, lihat CloneSecurityGroup.

Ketika saya mengkloning grup keamanan ke proyek atau wilayah lain, apakah CVM yang dikaitkan dengan grup keamanan juga akan dikloning?

Tidak. Hanya aturan masuk dan keluar grup keamanan yang dikloning. Anda perlu mengaitkan CVM lagi setelah kloning.