Penyeimbang Beban Gateway

Penyeimbang Beban Elastis

Penyeimbang Beban Elastis: Penyeimbang Beban Gateway

Table of Contents

Apa itu Gateway Load Balancer?

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas masuk Anda ke beberapa target, dalam satu atau beberapa Availability Zone. Ini memantau kesehatan target terdaftarnya, dan mengarahkan lalu lintas hanya ke target yang sehat. Elastic Load Balancing menskalakan load balancer Anda saat lalu lintas masuk Anda berubah seiring waktu. Ini dapat secara otomatis menskalakan sebagian besar beban kerja.

Elastic Load Balancing mendukung penyeimbang beban berikut: Application Load Balancer, Penyeimbang Beban Jaringan, Gateway Load Balancer, dan Classic Load Balancer. Anda dapat memilih jenis load balancer yang paling sesuai dengan kebutuhan Anda. Panduan ini membahas Gateway Load Balancers. Untuk informasi selengkapnya tentang load balancer lainnya, lihat Panduan Pengguna untuk Application Load Balancer, Panduan Pengguna untuk Network Load Balancer, dan Panduan Pengguna untuk Classic Load Balancer.

Ikhtisar Load Balancer Gateway

Penyeimbang Beban Gateway memungkinkan Anda untuk men-deploy, menskalakan, dan mengelola peralatan virtual, seperti firewall, sistem deteksi dan pencegahan intrusi, dan sistem inspeksi paket mendalam. Penyeimbang Beban Gateway menggabungkan gateway jaringan transparan (yaitu, satu titik masuk dan keluar untuk semua lalu lintas) dan mendistribusikan lalu lintas sambil menskalakan peralatan virtual Anda dengan permintaan.

Penyeimbang Beban Gateway beroperasi pada lapisan ketiga model Open Systems Interconnection (OSI), yaitu lapisan jaringan. Penyeimbang Beban Gateway mendengarkan semua paket IP di semua port dan meneruskan lalu lintas ke grup target yang ditentukan dalam aturan listener. Ini mempertahankan kelengketan aliran ke alat target tertentu menggunakan 5-tuple (default), 3-tuple, atau 2-tuple. Load Balancer Gateway dan instans alat virtual terdaftarnya bertukar lalu lintas aplikasi menggunakan protokol GENEVE pada port 6081.

Penyeimbang Beban Gateway menggunakan titik akhir Penyeimbang Beban Gateway untuk bertukar lalu lintas dengan aman melintasi batas VPC. Titik akhir Penyeimbang Beban Gateway adalah VPC endpoint yang menyediakan konektivitas privat antara peralatan virtual di dalam VPC penyedia layanan dan server aplikasi di dalam VPC konsumen layanan. Anda men-deploy Penyeimbang Beban Gateway di VPC yang sama dengan peralatan virtual. Anda mendaftarkan peralatan virtual dengan grup target untuk Penyeimbang Beban Gateway.

Lalu lintas ke dan dari titik akhir Load Balancer Gateway dikonfigurasi menggunakan tabel rute. Lalu lintas mengalir dari VPC konsumen layanan melalui titik akhir Load Balancer Gateway ke Load Balancer Gateway di VPC penyedia layanan, dan kemudian kembali ke VPC konsumen layanan. Anda harus membuat titik akhir Load Balancer Gateway dan server aplikasi dalam subnet yang berbeda. Ini memungkinkan Anda untuk mengkonfigurasi titik akhir Load Balancer Gateway sebagai lompatan berikutnya dalam tabel rute untuk subnet aplikasi.

Untuk informasi selengkapnya, lihat Mengakses peralatan virtual melalui AWS PrivateLinkAWS PrivateLink Panduan.

Vendor alat

Anda bertanggung jawab untuk memilih dan memenuhi syarat perangkat lunak dari vendor alat. Anda harus mempercayai perangkat lunak alat untuk memeriksa atau memodifikasi lalu lintas dari penyeimbang beban. Vendor alat yang terdaftar sebagai Elastic Load Balancing Partners telah mengintegrasikan dan memenuhi syarat perangkat lunak alat mereka. AWS Anda dapat menempatkan tingkat kepercayaan yang lebih tinggi pada perangkat lunak alat dari vendor dalam daftar ini. Namun, AWS tidak menjamin keamanan atau keandalan perangkat lunak dari vendor-vendor ini.

Memulai

Untuk membuat Load Balancer Gateway menggunakan AWS Management Console, lihat. Memulai Untuk membuat Load Balancer Gateway menggunakan AWS Command Line Interface, lihat. Memulai menggunakan CLI

Harga

Dengan penyeimbang beban, Anda hanya membayar apa yang Anda gunakan. Untuk informasi lebih lanjut, lihat Harga Elastic Load Balancing?

Memulai dengan Gateway Load Balancers

Gateway Load Balancers memudahkan penerapan, skala, dan pengelolaan peralatan virtual pihak ketiga, seperti peralatan keamanan.

Dalam tutorial ini, kita akan menerapkan sistem inspeksi menggunakan Load Balancer Gateway dan titik akhir Gateway Load Balancer.

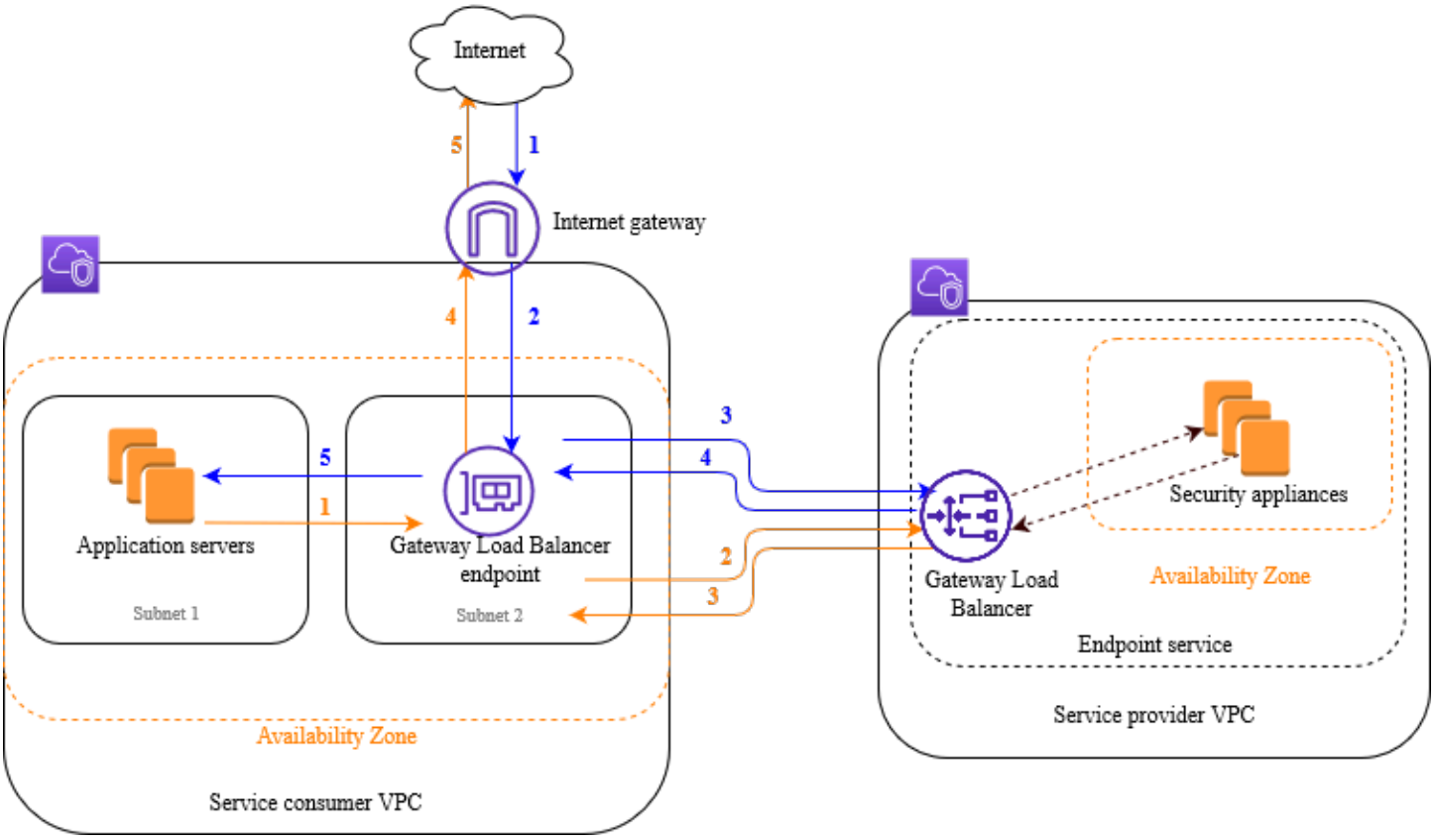
Daftar Isi

Gambaran Umum

Endpoint Load Balancer Gateway adalah titik akhir VPC yang menyediakan konektivitas pribadi antara peralatan virtual di VPC penyedia layanan, dan server aplikasi di VPC konsumen layanan. Load Balancer Gateway digunakan di VPC yang sama dengan peralatan virtual. Peralatan ini terdaftar sebagai kelompok sasaran Gateway Load Balancer.

Server aplikasi berjalan dalam satu subnet (subnet tujuan) di VPC konsumen layanan, sedangkan titik akhir Load Balancer Gateway berada di subnet lain dari VPC yang sama. Semua lalu lintas yang memasuki VPC konsumen layanan melalui gateway internet pertama-tama dialihkan ke titik akhir Gateway Load Balancer dan kemudian dirutekan ke subnet tujuan.

Demikian pula, semua lalu lintas yang meninggalkan server aplikasi (subnet tujuan) dirutekan ke titik akhir Gateway Load Balancer sebelum dirutekan kembali ke internet. Diagram jaringan berikut adalah representasi visual tentang bagaimana titik akhir Load Balancer Gateway digunakan untuk mengakses layanan endpoint.



Item bernomor yang mengikuti, menyorot, dan menjelaskan elemen yang ditunjukkan pada gambar sebelumnya.

Lalu lintas dari internet ke aplikasi (panah biru):

1. Lalu lintas memasuki VPC konsumen layanan melalui gateway internet.
2. Lalu lintas dikirim ke titik akhir Load Balancer Gateway, sebagai akibat dari perutean ingress.
3. Lalu lintas dikirim ke Load Balancer Gateway, yang mendistribusikan lalu lintas ke salah satu peralatan keamanan.
4. Lalu lintas dikirim kembali ke titik akhir Load Balancer Gateway setelah diperiksa oleh alat keamanan.
5. Lalu lintas dikirim ke server aplikasi (subnet tujuan).

Lalu lintas dari aplikasi ke internet (panah oranye):

1. Lalu lintas dikirim ke titik akhir Load Balancer Gateway sebagai hasil dari rute default yang dikonfigurasi pada subnet server aplikasi.

2. Lalu lintas dikirim ke Load Balancer Gateway, yang mendistribusikan lalu lintas ke salah satu peralatan keamanan.
3. Lalu lintas dikirim kembali ke titik akhir Load Balancer Gateway setelah diperiksa oleh alat keamanan.
4. Lalu lintas dikirim ke gateway internet berdasarkan konfigurasi tabel rute.
5. Lalu lintas dialihkan kembali ke internet.

Perutean

Tabel rute untuk gateway internet harus memiliki entri yang mengarahkan lalu lintas yang ditujukan untuk server aplikasi ke titik akhir Load Balancer Gateway. Untuk menentukan titik akhir Load Balancer Gateway, gunakan ID titik akhir VPC. Contoh berikut menunjukkan rute untuk konfigurasi dualstack.

Tujuan	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
Subnet 1 IPv4 CIDR	*vpc-endpoint-id*
Subnet 1 IPv6 CIDR	*vpc-endpoint-id*

Tabel rute untuk subnet dengan server aplikasi harus memiliki entri yang merutekan semua lalu lintas dari server aplikasi ke titik akhir Load Balancer Gateway.

Tujuan	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabel rute untuk subnet dengan titik akhir Gateway Load Balancer harus merutekan lalu lintas yang kembali dari inspeksi ke tujuan akhirnya. Untuk lalu lintas yang berasal dari internet, rute lokal memastikan bahwa ia mencapai server aplikasi. Untuk lalu lintas yang berasal dari server aplikasi, tambahkan entri yang merutekan semua lalu lintas ke gateway internet.

Tujuan	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Prasyarat

- Pastikan VPC konsumen layanan memiliki setidaknya dua subnet untuk setiap Availability Zone yang berisi server aplikasi. Satu subnet adalah untuk titik akhir Gateway Load Balancer, dan yang lainnya untuk server aplikasi.
- Load Balancer Gateway dan targetnya bisa berada di subnet yang sama.
- Anda tidak dapat menggunakan subnet yang dibagikan dari akun lain untuk menyebarkan Load Balancer Gateway.
- Luncurkan setidaknya satu instance alat keamanan di setiap subnet alat keamanan di VPC penyedia layanan. Grup keamanan untuk instance ini harus mengizinkan lalu lintas UDP di port 6081.

Langkah 1: Buat Load Balancer Gateway

Gunakan prosedur berikut untuk membuat penyeimbang beban, pendengar, dan grup target Anda.

Untuk membuat load balancer, listener, dan grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Buat Penyeimbang Beban.

4. Di bawah Load Balancer Gateway, pilih Buat.
5. Konfigurasi dasar
   a. Untuk Name, masukkan nama untuk penyeimbang beban Anda.
   b. Untuk jenis alamat IP, pilih IPv4 untuk mendukung alamat IPv4 saja atau Dualstack untuk mendukung alamat IPv4 dan IPv6.
6. Pemetaan jaringan
   a. Untuk VPC, pilih penyedia layanan VPC.
   b. Untuk Pemetaan, pilih semua Availability Zone tempat Anda meluncurkan instance alat keamanan, dan satu subnet per Availability Zone.
7. Perutean pendengar IP
   a. Untuk tindakan Default, pilih grup target yang ada untuk menerima lalu lintas. Kelompok sasaran ini harus menggunakan protokol GENEVE.

      Jika Anda tidak memiliki grup target, pilih Buat grup target, yang membuka tab baru di browser Anda. Pilih jenis target, masukkan nama untuk grup target, dan pertahankan protokol GENEVE. Pilih VPC dengan instans alat keamanan Anda. Ubah pengaturan pemeriksaan kesehatan sesuai kebutuhan, dan tambahkan tag apa pun yang Anda butuhkan. Pilih Selanjutnya. Anda dapat mendaftarkan instance alat keamanan Anda dengan grup target sekarang, atau setelah Anda menyelesaikan prosedur ini. Pilih Buat grup target dan kemudian kembali ke tab browser sebelumnya.
   b. (Opsional) Perluas tag Listener dan tambahkan tag yang Anda butuhkan.
8. (Opsional) Perluas tag penyeimbang beban dan tambahkan tag yang Anda butuhkan.
9. Pilih Buat Penyeimbang Beban.

Langkah 2: Buat layanan titik akhir Load Balancer Gateway

Gunakan prosedur berikut untuk membuat layanan endpoint menggunakan Load Balancer Gateway Anda.

Untuk membuat layanan titik akhir Load Balancer Gateway

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.

3. Pilih Create endpoint service dan lakukan hal berikut:

    a. Untuk jenis Load balancer, pilih Gateway.
    b. Untuk penyeimbang beban yang tersedia, pilih Load Balancer Gateway Anda.
    c. Untuk Memerlukan penerimaan untuk titik akhir, pilih Penerimaan yang diperlukan untuk menerima permintaan koneksi ke layanan Anda secara manual. Jika tidak, mereka secara otomatis diterima.
    d. Untuk jenis alamat IP yang Didukung, lakukan salah satu hal berikut:

        - Pilih IPv4 - Aktifkan layanan endpoint untuk menerima permintaan IPv4.
        - Pilih IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv6.
        - Pilih IPv4 dan IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv4 dan IPv6.

    e. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
    f. Pilih Buat. Perhatikan nama layanan; Anda akan membutuhkannya saat membuat titik akhir.
4. Pilih layanan endpoint baru dan pilih Actions, Allow principals. Masukkan ARN konsumen layanan yang diizinkan untuk membuat titik akhir ke layanan Anda. Konsumen layanan dapat menjadi pengguna, peran IAM, atau Akun AWS. Pilih Izinkan prinsipal.

Langkah 3: Buat titik akhir Load Balancer Gateway

Gunakan prosedur berikut untuk membuat titik akhir Load Balancer Gateway yang terhubung ke layanan titik akhir Load Balancer Gateway Anda. Titik akhir Load Balancer Gateway bersifat zonal. Kami menyarankan Anda membuat satu titik akhir Load Balancer Gateway per zona. Untuk informasi selengkapnya, lihat Mengakses peralatan virtual melalui AWS PrivateLinkAWS PrivateLink Panduan.

Untuk membuat titik akhir Load Balancer Gateway

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik Akhir.
3. Pilih Buat titik akhir dan lakukan hal berikut:

    a. Untuk kategori Layanan, pilih Layanan endpoint lainnya.
    b. Untuk nama Layanan, masukkan nama layanan yang Anda catat sebelumnya, lalu pilih Verifikasi layanan.

c. Untuk VPC, pilih VPC konsumen layanan.

d. Untuk Subnet, pilih subnet untuk titik akhir Gateway Load Balancer.

e. Untuk jenis alamat IP, pilih dari opsi berikut:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

f. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.

g. Pilih Buat Titik Akhir. Status awal adalah `pending acceptance`.

Untuk menerima permintaan koneksi titik akhir, gunakan prosedur berikut.

1. Di panel navigasi, pilih Layanan titik akhir.
2. Pilih layanan endpoint.
3. Dari tab Koneksi titik akhir, pilih koneksi titik akhir.
4. Untuk menerima permintaan koneksi, pilih Tindakan, Terima permintaan koneksi titik akhir. Saat diminta konfirmasi, masukkan **`accept`** lalu pilih Terima.

Langkah 4: Konfigurasikan perutean

Konfigurasikan tabel rute untuk VPC konsumen layanan sebagai berikut. Hal ini memungkinkan peralatan keamanan untuk melakukan pemeriksaan keamanan pada lalu lintas masuk yang ditujukan untuk server aplikasi.

Untuk mengkonfigurasi routing

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute.
3. Pilih tabel rute untuk gateway internet dan lakukan hal berikut:

a. Pilih Tindakan, Sunting rute.

b. Pilih Tambahkan rute. Untuk Tujuan, masukkan blok IPv4 CIDR subnet untuk server aplikasi. Untuk Target, pilih titik akhir VPC.

c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan blok IPv6 CIDR subnet untuk server aplikasi. Untuk Target, pilih titik akhir VPC.

d. Pilih Simpan perubahan.

4. Pilih tabel rute untuk subnet dengan server aplikasi dan lakukan hal berikut:

a. Pilih Tindakan, Sunting rute.

b. Pilih Tambahkan rute. Untuk Tujuan, masukkan**`0.0.0.0/0`**. Untuk Target, pilih titik akhir VPC.

c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan**`::/0`**. Untuk Target, pilih titik akhir VPC.

d. Pilih Simpan perubahan.

5. Pilih tabel rute untuk subnet dengan titik akhir Gateway Load Balancer, dan lakukan hal berikut:

a. Pilih Tindakan, Sunting rute.

b. Pilih Tambahkan rute. Untuk Tujuan, masukkan**`0.0.0.0/0`**. Untuk Target, pilih gateway internet.

c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan**`::/0`**. Untuk Target, pilih gateway internet.

d. Pilih Simpan perubahan.

Memulai dengan Gateway Load Balancers menggunakan AWS CLI

Gateway Load Balancers memudahkan penerapan, penskalaan, dan pengelolaan peralatan virtual pihak ketiga, seperti peralatan keamanan.

Dalam tutorial ini, kita akan menerapkan sistem inspeksi menggunakan Gateway Load Balancer dan titik akhir Gateway Load Balancer.

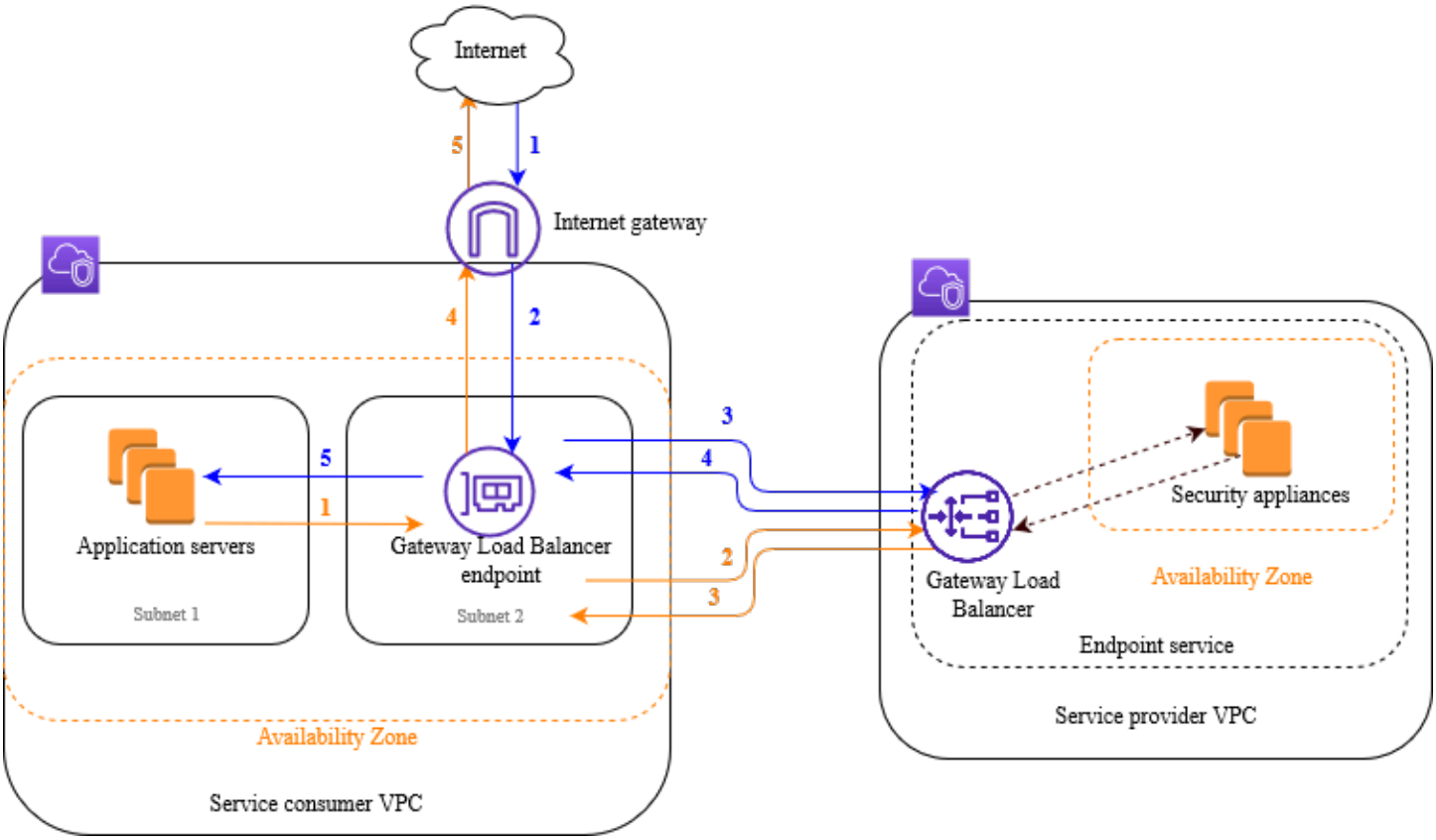
Daftar Isi

Gambaran Umum

Endpoint Gateway Load Balancer adalah titik akhir VPC yang menyediakan konektivitas pribadi antara peralatan virtual di penyedia layanan VPC, dan server aplikasi di VPC konsumen layanan. Gateway Load Balancer digunakan di VPC yang sama dengan peralatan virtual. Peralatan ini terdaftar sebagai kelompok target Gateway Load Balancer.

Server aplikasi berjalan dalam satu subnet (subnet tujuan) di VPC konsumen layanan, sedangkan endpoint Gateway Load Balancer berada di subnet lain dari VPC yang sama. Semua lalu lintas yang memasuki layanan konsumen VPC melalui gateway internet pertama dialihkan ke endpoint Gateway Load Balancer dan kemudian dialihkan ke subnet tujuan.

Demikian pula, semua lalu lintas yang meninggalkan server aplikasi (subnet tujuan) dialihkan ke titik akhir Gateway Load Balancer sebelum dialihkan kembali ke internet. Diagram jaringan berikut adalah representasi visual tentang bagaimana titik akhir Gateway Load Balancer digunakan untuk mengakses layanan endpoint.



Item bernomor yang mengikuti, menyorot dan menjelaskan elemen yang ditunjukkan pada gambar sebelumnya.

Lalu lintas dari internet ke aplikasi (panah biru):

1. Lalu lintas memasuki layanan konsumen VPC melalui gateway internet.
2. Lalu lintas dikirim ke titik akhir Gateway Load Balancer, sebagai hasil dari perutean masuknya.
3. Lalu lintas dikirim ke Gateway Load Balancer, yang mendistribusikan lalu lintas ke salah satu peralatan keamanan.
4. Lalu lintas dikirim kembali ke titik akhir Gateway Load Balancer setelah diperiksa oleh alat keamanan.
5. Lalu lintas dikirim ke server aplikasi (subnet tujuan).

Lalu lintas dari aplikasi ke internet (panah oranye):

1. Lalu lintas dikirim ke titik akhir Gateway Load Balancer sebagai hasil dari rute default yang dikonfigurasi pada subnet server aplikasi.

2. Lalu lintas dikirim ke Gateway Load Balancer, yang mendistribusikan lalu lintas ke salah satu peralatan keamanan.
3. Lalu lintas dikirim kembali ke titik akhir Gateway Load Balancer setelah diperiksa oleh alat keamanan.
4. Lalu lintas dikirim ke gateway internet berdasarkan konfigurasi tabel rute.
5. Lalu lintas dialihkan kembali ke internet.

Perutean

Tabel rute untuk gateway internet harus memiliki entri yang merutekan lalu lintas yang ditujukan untuk server aplikasi ke titik akhir Gateway Load Balancer. Untuk menentukan titik akhir Gateway Load Balancer, gunakan ID titik akhir VPC. Contoh berikut menunjukkan rute untuk konfigurasi dualstack.

Tujuan	Target
VPC IPv4	Lokal:
VPC IPv6	Lokal:
Subnet 1 IPv4 CIDR	*vpc-endpoint-id*
Subnet 1 IPv6 CIDR	*vpc-endpoint-id*

Tabel rute untuk subnet dengan server aplikasi harus memiliki entri yang merutekan semua lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer.

Tujuan	Target
VPC IPv4	Lokal:
VPC IPv6	Lokal:
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabel rute untuk subnet dengan titik akhir Gateway Load Balancer harus merutekan lalu lintas yang kembali dari inspeksi ke tujuan akhirnya. Untuk lalu lintas yang berasal dari internet, rute lokal memastikan bahwa ia mencapai server aplikasi. Untuk lalu lintas yang berasal dari server aplikasi, tambahkan entri yang merutekan semua lalu lintas ke gateway internet.

Tujuan	Target
VPC IPv4	Lokal:
VPC IPv6	Lokal:
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Prasyarat

- Instal AWS CLI atau perbarui ke versi saat ini AWS CLI jika Anda menggunakan versi yang tidak mendukung Gateway Load Balancers. Untuk informasi selengkapnya, lihat Menginstal AWS Command Line Interface dalam Panduan Pengguna AWS Command Line Interface.
- Pastikan bahwa konsumen layanan VPC memiliki setidaknya dua subnet untuk setiap Availability Zone yang berisi server aplikasi. Satu subnet adalah untuk endpoint Gateway Load Balancer, dan yang lainnya adalah untuk server aplikasi.
- Pastikan penyedia layanan VPC memiliki setidaknya dua subnet untuk setiap Availability Zone yang berisi instans alat keamanan. Satu subnet adalah untuk Gateway Load Balancer, dan yang lainnya untuk instance.
- Luncurkan setidaknya satu instans alat keamanan di setiap subnet alat keamanan di penyedia layanan VPC. Grup keamanan untuk instance ini harus mengizinkan lalu lintas UDP pada port 6081.

Langkah 1: Buat Gateway Load Balancer dan daftar target

Gunakan prosedur berikut untuk membuat penyeimbang muatan, listener, dan grup target, dan untuk mendaftarkan instance alat keamanan Anda sebagai target.

Untuk membuat Gateway Load Balancer dan mendaftarkan target

1. Gunakan create-load-balancerperintah untuk membuat load balancer tipe`gateway`. Anda dapat menentukan satu subnet untuk setiap Availability Zone tempat Anda meluncurkan instans alat keamanan.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer --type gateway --
   subnets provider-subnet-id
   ```

   Defaultnya adalah untuk mendukung alamat IPv4 saja. Untuk mendukung alamat IPv4 dan IPv6, tambahkan opsi. `--ip-address-type dualstack`

   Output mencakup Amazon Resource Name (ARN) dari load balancer, dengan format yang ditunjukkan dalam contoh berikut.

   ```
   arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/gwy/my-load-
   balancer/1234567890123456
   ```

2. Gunakan create-target-groupperintah untuk membuat grup target, menentukan penyedia layanan VPC tempat Anda meluncurkan instance Anda.

   ```
   aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 --
   vpc-id provider-vpc-id
   ```

   Output termasuk ARN dari kelompok target, dengan format berikut.

   ```
   arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
   targets/0123456789012345
   ```

3. Gunakan perintah register-targets untuk mendaftarkan instans Anda dengan grup target Anda.

   ```
   aws elbv2 register-targets --target-group-arn targetgroup-arn --targets
    Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
   ```

4. Gunakan perintah create-listener untuk membuat listener untuk load balancer Anda dengan aturan default yang meneruskan permintaan ke grup target Anda.

   ```
   aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --default-actions
    Type=forward,TargetGroupArn=targetgroup-arn
   ```

Output berisi ARN pendengar, dengan format berikut.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/gwy/my-load-
balancer/1234567890123456/abc1234567890123
```

5. (Opsional) Anda dapat memverifikasi kesehatan target terdaftar untuk grup target Anda menggunakan describe-target-healthperintah berikut.

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Langkah 2: Buat titik akhir Gateway Load Balancer

Gunakan prosedur berikut untuk membuat titik akhir Gateway Load Balancer. Titik akhir Gateway Load Balancer bersifat zonal. Kami menyarankan Anda membuat satu titik akhir Gateway Load Balancer per zona. Untuk informasi selengkapnya, lihat Mengakses peralatan virtual melalui AWS PrivateLink.

Untuk membuat titik akhir Gateway Load Balancer

1. Gunakan vpc-endpoint-service-configuration perintah create- untuk membuat konfigurasi layanan endpoint menggunakan Gateway Load Balancer Anda.

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-
arns loadbalancer-arn --no-acceptance-required
```

   Untuk mendukung alamat IPv4 dan IPv6, tambahkan opsi. `--supported-ip-address-types ipv4 ipv6`

   Output berisi ID layanan (misalnya, vpce-svc-12345678901234567) dan nama layanan (misalnya, com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567).

2. Gunakan vpc-endpoint-service-permissions perintah modify- untuk memungkinkan konsumen layanan membuat endpoint ke layanan Anda. Konsumen layanan dapat berupa pengguna, peran IAM, atauAkun AWS. Contoh berikut menambahkan izin untuk yang ditentukanAkun AWS.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-
svc-12345678901234567 --add-allowed-principals arn:aws:iam::123456789012:root
```

3. Gunakan perintah create-vpc-endpoint untuk membuat endpoint Gateway Load Balancer untuk layanan Anda.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --service-name com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpc-id --subnet-ids consumer-subnet-id
```

   Untuk mendukung alamat IPv4 dan IPv6, tambahkan opsi. `--ip-address-type dualstack`

   Output berisi ID titik akhir Gateway Load Balancer (misalnya, vpce-01234567890abcdef).

Langkah 3: Konfigurasikan perutean

Konfigurasikan tabel rute untuk VPC konsumen layanan sebagai berikut. Hal ini memungkinkan peralatan keamanan untuk melakukan pemeriksaan keamanan pada lalu lintas masuk yang ditujukan untuk server aplikasi.

Untuk mengkonfigurasi routing

1. Gunakan perintah create-route untuk menambahkan entri ke tabel rute untuk gateway internet yang merutekan lalu lintas yang ditujukan untuk server aplikasi ke titik akhir Gateway Load Balancer.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv4 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

   Jika Anda mendukung IPv6, tambahkan rute berikut.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv6 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

2. Gunakan perintah create-route untuk menambahkan entri ke tabel rute untuk subnet dengan server aplikasi yang merutekan semua lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block 0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef
```

   Jika Anda mendukung IPv6, tambahkan rute berikut.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block ::/0
 --vpc-endpoint-id vpce-01234567890abcdef
```

3. Gunakan perintah create-route untuk menambahkan entri ke tabel rute untuk subnet dengan titik akhir Gateway Load Balancer yang merutekan semua lalu lintas yang berasal dari server aplikasi ke gateway internet.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-01234567890abcdef
```

   Jika Anda mendukung IPv6, tambahkan rute berikut.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block ::/0 --
gateway-id igw-01234567890abcdef
```

4. Ulangi untuk setiap tabel rute subnet aplikasi di setiap zona.

Penyeimbang Beban Gateway

Gunakan Load Balancer Gateway untuk menyebarkan dan mengelola armada peralatan virtual yang mendukung protokol GENEVE.

Load Balancer Gateway beroperasi pada lapisan ketiga model Open Systems Interconnection (OSI). Ini mendengarkan semua paket IP di semua port dan meneruskan lalu lintas ke grup target yang ditentukan dalam aturan pendengar, menggunakan protokol GENEVE pada port 6081.

Anda dapat menambah atau menghapus target dari penyeimbang beban saat kebutuhan Anda berubah, tanpa mengganggu aliran permintaan secara keseluruhan. Elastic Load Balancing menskalakan penyeimbang beban Anda saat lalu lintas ke aplikasi Anda berubah seiring waktu. Elastic Load Balancing dapat menskalakan sebagian besar beban kerja secara otomatis.

Daftar Isi

Keadaan penyeimbang beban

Load Balancer Gateway dapat berada di salah satu status berikut:

`provisioning`

Load Balancer Gateway sedang disiapkan.

`active`

Load Balancer Gateway sepenuhnya diatur dan siap untuk mengarahkan lalu lintas.

`failed`

Load Balancer Gateway tidak dapat diatur.

Jenis alamat IP

Anda dapat mengatur jenis alamat IP yang dapat digunakan server aplikasi untuk mengakses Gateway Load Balancers Anda.

Gateway Load Balancers mendukung jenis alamat IP berikut:

`ipv4`

Hanya IPv4 yang didukung.

`dualstack`

IPv4 dan IPv6 didukung.

Pertimbangan

- Virtual private cloud (VPC) dan subnet yang Anda tentukan untuk penyeimbang beban harus memiliki blok CIDR IPv6 terkait.
- Tabel rute untuk subnet di VPC konsumen layanan harus merutekan lalu lintas IPv6, dan ACL jaringan untuk subnet ini harus memungkinkan lalu lintas IPv6.
- Load Balancer Gateway merangkum lalu lintas klien IPv4 dan IPv6 dengan header IPv4 GENEVE dan mengirimkannya ke alat. Alat ini merangkum lalu lintas klien IPv4 dan IPv6 dengan header IPv4 GENEVE dan mengirimkannya kembali ke Load Balancer Gateway.

Untuk informasi selengkapnya tentang jenis alamat IP, lihatJenis alamat IP untuk Load Balancer Gateway Anda.

Atribut penyeimbang beban

Berikut ini adalah atribut load balancer untuk Gateway Load Balancers:

`deletion_protection.enabled`

Menunjukkan apakah Perlindungan penghapusan diaktifkan. Default-nya adalah `false`.

`load_balancing.cross_zone.enabled`

Menunjukkan apakah penyeimbangan beban lintas zona diaktifkan. Default-nya adalah `false`.

Zona Ketersediaan

Saat membuat Load Balancer Gateway, Anda mengaktifkan satu atau beberapa Availability Zone, dan menentukan subnet yang sesuai dengan setiap zona. Saat Anda mengaktifkan beberapa Availability Zone, ini memastikan bahwa penyeimbang beban dapat terus merutekan lalu lintas meskipun Availability Zone menjadi tidak tersedia. Subnet yang Anda tentukan masing-masing harus memiliki setidaknya 8 alamat IP yang tersedia. Subnet tidak dapat dihapus setelah penyeimbang beban dibuat. Untuk menghapus subnet, Anda harus membuat penyeimbang beban baru.

Unit transmisi maksimum jaringan (MTU)

Unit transmisi maksimum (MTU) adalah ukuran paket data terbesar yang dapat ditransmisikan melalui jaringan. Antarmuka Gateway Load Balancer MTU mendukung paket hingga 8.500 byte. Paket dengan ukuran lebih besar dari 8500 byte yang tiba di antarmuka Gateway Load Balancer dijatuhkan.

Load Balancer Gateway merangkum lalu lintas IP dengan header GENEVE dan meneruskannya ke alat. Proses enkapsulasi GENEVE menambahkan 64 byte ke paket asli. Oleh karena itu, untuk mendukung paket hingga 8.500 byte, pastikan bahwa pengaturan MTU alat Anda mendukung paket minimal 8.564 byte.

Gateway Load Balancer tidak mendukung fragmentasi IP. Selain itu, Gateway Load Balancer tidak menghasilkan pesan ICMP “Destination Unreachable: fragmentation needed and DF set”. Karena ini, Path MTU Discovery (PMTUD) tidak didukung.

Perlindungan penghapusan

Untuk mencegah Load Balancer Gateway Anda dihapus secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghapusan. Secara default, perlindungan penghapusan dinonaktifkan.

Jika Anda mengaktifkan perlindungan penghapusan untuk Load Balancer Gateway, Anda harus menonaktifkannya sebelum dapat menghapus Load Balancer Gateway.

Untuk mengaktifkan perlindungan penghapusan menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Load Balancer Gateway.
4. Pilih Tindakan, Edit atribut.
5. Pada halaman Edit load balancer attributes, pilih Enable untuk Delete Protection, lalu pilih Simpan.

Untuk menonaktifkan perlindungan penghapusan menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Load Balancer Gateway.
4. Pilih Tindakan, Edit atribut.
5. Pada halaman Edit load balancer attributes, hapus Enable untuk Delete Protection, lalu pilih Simpan.

Untuk mengaktifkan atau menonaktifkan perlindungan penghapusan menggunakan AWS CLI

Gunakan perintah modify-load-balancer-attributes dengan atribut `deletion_protection.enabled`.

Penyeimbangan beban lintas zona

Secara default, setiap simpul penyeimbang beban mendistribusikan lalu lintas di target yang terdaftar di Availability Zone saja. Jika Anda mengaktifkan penyeimbangan beban lintas zona, setiap node Load Balancer Gateway mendistribusikan lalu lintas di seluruh target terdaftar di semua Availability

Zone yang diaktifkan. Untuk informasi lebih lanjut, lihat Penyeimbang beban lintas zona di Panduan Pengguna Elastic Load Balancing.

Untuk mengaktifkan penyeimbangan beban lintas zona menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Load Balancer Gateway.
4. Pilih Tindakan, Edit atribut.
5. Pada halaman Edit atribut penyeimbang beban, pilih Aktifkan untuk Penyeimbangan Beban Lintas Zona, lalu pilih Simpan.

Untuk mengaktifkan penyeimbangan beban lintas zona menggunakan AWS CLI

Gunakan perintah modify-load-balancer-attributes dengan atribut `load_balancing.cross_zone.enabled`.

Aliran asimetris

Gateway Load Balancers mendukung aliran asimetris ketika penyeimbang beban memproses paket aliran awal dan paket aliran respons tidak dirutekan melalui penyeimbang beban. Perutean asimetris tidak disarankan, karena dapat mengakibatkan penurunan kinerja jaringan. Gateway Load Balancer tidak mendukung aliran asimetris ketika penyeimbang beban tidak memproses paket aliran awal tetapi paket aliran respons dialihkan melalui penyeimbang beban.

Batas waktu idle

Gateway Load Balancers mendukung batas waktu idle untuk aliran TCP, dan non-TCP.

- Untuk aliran TCP, batas waktu idle adalah 350 detik.
- Untuk aliran non-TCP, batas waktu idle adalah 120 detik.

Catatan: Nilai batas waktu idle untuk Gateway Load Balancers bersifat statis dan tidak dapat diubah.

Membuat Gateway Load Balancer

Load Balancer Gateway mengambil permintaan dari klien dan mendistribusikannya ke seluruh target dalam grup target, seperti instans EC2.

Untuk membuat Load Balancer Gateway menggunakan AWS Management Console, selesaikan tugas-tugas berikut.

Tugas

- Prasyarat
- Buat penyeimbang beban
- Langkah penting selanjutnya

Atau, untuk membuat Load Balancer Gateway menggunakan AWS CLI, lihat. Memulai menggunakan CLI

Prasyarat

Sebelum memulai, pastikan bahwa virtual private cloud (VPC) untuk Load Balancer Gateway Anda memiliki setidaknya satu subnet di setiap Availability Zone tempat Anda memiliki target.

Buat penyeimbang beban

Gunakan prosedur berikut untuk membuat Load Balancer Gateway Anda. Berikan informasi konfigurasi dasar untuk penyeimbang beban Anda, seperti nama dan jenis alamat IP. Kemudian berikan informasi tentang jaringan Anda, dan pendengar yang mengarahkan lalu lintas ke grup target Anda. Gateway Load Balancers memerlukan grup target yang menggunakan protokol GENEVE.

Untuk membuat penyeimbang beban dan pendengar menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Buat Penyeimbang Beban.
4. Di bawah Load Balancer Gateway, pilih Buat.
5. Konfigurasi dasar

    a. Untuk Name, masukkan nama untuk penyeimbang beban Anda. Sebagai contoh, **`my-glb`**. Nama Load Balancer Gateway Anda harus unik dalam rangkaian penyeimbang beban untuk

Wilayah. Ini dapat memiliki maksimal 32 karakter, hanya dapat berisi karakter alfanumerik dan tanda hubung, dan tidak boleh dimulai atau diakhiri dengan tanda hubung.

b. Untuk jenis alamat IP, pilih IPv4 untuk mendukung alamat IPv4 saja atau Dualstack untuk mendukung alamat IPv4 dan IPv6.

6. Pemetaan jaringan

a. Untuk VPC, pilih penyedia layanan VPC.

b. Untuk Pemetaan, pilih semua Availability Zone tempat Anda meluncurkan instance alat keamanan, dan subnet publik terkait.

7. Perutean pendengar IP

a. Untuk tindakan Default, pilih grup target untuk menerima lalu lintas. Jika Anda tidak memiliki grup target, pilih Buat grup target. Untuk informasi selengkapnya, lihat Buat grup target.

b. (Opsional) Perluas tag Listener dan tambahkan tag yang Anda butuhkan.

8. (Opsional) Perluas tag penyeimbang beban dan tambahkan tag yang Anda butuhkan.

9. Tinjau konfigurasi Anda, lalu pilih Buat penyeimbang beban.

Langkah penting selanjutnya

Setelah membuat penyeimbang beban, verifikasi bahwa instans EC2 Anda telah lulus pemeriksaan kesehatan awal. Untuk menguji penyeimbang beban Anda, Anda harus membuat titik akhir Load Balancer Gateway dan memperbarui tabel rute Anda untuk membuat titik akhir Gateway Load Balancer menjadi lompatan berikutnya. Konfigurasi ini diatur dalam konsol VPC Amazon. Untuk informasi selengkapnya, lihat tutorial Memulai.

Jenis alamat IP untuk Load Balancer Gateway Anda

Anda dapat mengonfigurasi Load Balancer Gateway Anda sehingga server aplikasi dapat mengakses penyeimbang beban Anda hanya menggunakan alamat IPv4, atau menggunakan alamat IPv4 dan IPv6 (dualstack). Load balancer berkomunikasi dengan target berdasarkan jenis alamat IP dari kelompok target. Untuk informasi selengkapnya, lihat Jenis alamat IP.

Untuk menetapkan jenis alamat IP pada penciptaan

Mengkonfigurasi pengaturan seperti yang dijelaskan di ???.

Untuk memperbarui jenis alamat IP menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih penyeimbang beban.
4. Pilih Actions, Edit IP address type.
5. Untuk IP address type, pilih ipv4 untuk mendukung alamat IPv4 saja atau dualstack untuk mendukung alamat IPv4 and IPv6.
6. Pilih Simpan.

Untuk memperbarui jenis alamat IP menggunakan AWS CLI

Gunakan perintah set-ip-address-type.

Tag untuk Load Balancer Gateway Anda

Tag membantu Anda mengategorikan penyeimbang beban dengan cara yang berbeda, misalnya berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap penyeimbang beban. Kunci tag harus unik untuk setiap Load Balancer Gateway. Jika Anda menambahkan tag dengan kunci yang sudah terkait dengan penyeimbang beban, kunci akan memperbarui nilai tag tersebut.

Setelah selesai dengan tag, Anda dapat menghapusnya dari Load Balancer Gateway Anda.

Pembatasan

- Jumlah maksimum tanda per sumber daya—50
- Panjang kunci maksimum – 127 karakter Unicode
- Panjang nilai maksimum – 255 karakter Unicode
- Kunci dan nilai tanda peka huruf besar dan kecil. Karakter yang diperbolehkan adalah: huruf, spasi, dan angka yang dapat mewakili dalam UTF-8, serta karakter berikut: + - = . _ : / @. _:/@. Jangan gunakan spasi terkemuka atau paling belakang.
- Jangan gunakan `aws:` awalan dalam nama atau nilai tag Anda karena itu dicadangkan untuk AWS digunakan. Anda tidak dapat mengedit atau menghapus nama atau nilai tag dengan awalan ini. Tag dengan awalan ini tidak dihitung terhadap tag Anda per batas sumber daya.

Untuk memperbarui tag untuk Load Balancer Gateway menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Load Balancer Gateway.
4. Pilih Tag, Tambahkan/Edit Tag, lalu lakukan satu atau beberapa hal berikut:
   a. Untuk memperbarui tag, edit nilai Kunci dan Nilai.
   b. Untuk menambahkan tag baru, pilih Buat tag. Masukkan nilai untuk Kunci tag dan nilai.
   c. Untuk menghapus sebuah tag, pilih ikon hapus (X) di samping tag yang ingin dihapus.
5. Setelah Anda selesai menambahkan tag, pilih Simpan.

Untuk memperbarui tag untuk Load Balancer Gateway menggunakan AWS CLI

Penggunaan perintahPenambahan tagdanHapus tag.

Menghapus Load Balancer Gateway

Segera setelah Load Balancer Gateway Anda tersedia, Anda ditagih untuk setiap jam atau sebagian jam agar tetap berjalan. Ketika Anda tidak lagi membutuhkan Load Balancer Gateway, Anda dapat menghapusnya. Segera setelah Load Balancer Gateway dihapus, Anda berhenti mengeluarkan biaya untuk itu.

Anda tidak dapat menghapus Load Balancer Gateway jika sedang digunakan oleh layanan lain. Misalnya, jika Load Balancer Gateway dikaitkan dengan layanan titik akhir VPC, Anda harus menghapus konfigurasi layanan titik akhir sebelum dapat menghapus Load Balancer Gateway terkait.

Menghapus Load Balancer Gateway juga menghapus pendengarnya. Menghapus Load Balancer Gateway tidak memengaruhi target yang terdaftar. Misalnya, instans EC2 Anda terus berjalan dan masih terdaftar ke grup target mereka. Untuk menghapus grup target Anda, lihat Menghapus grup target.

Untuk menghapus n Gateway Load Balancer menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Load Balancer Gateway.

4. Pilih Tindakan, Hapus.
5. Ketika diminta konfirmasi, pilih Ya, Hapus.

Untuk menghapus Load Balancer Gateway menggunakan AWS CLI

Gunakan perintah delete-load-balancer.

Pendengar untuk Load Balancer Gateway Anda

Saat membuat Load Balancer Gateway, Anda menambahkan pendengar. Listener adalah proses memeriksa permintaan koneksi.

Pendengar untuk Gateway Load Balancers mendengarkan semua paket IP di semua port. Anda tidak dapat menentukan protokol atau port saat membuat listener untuk Load Balancer Gateway.

Saat membuat pendengar, Anda menentukan aturan untuk merutekan permintaan. Aturan ini meneruskan permintaan ke grup target yang ditentukan. Anda dapat memperbarui aturan listener untuk meneruskan permintaan ke grup target yang berbeda.

Untuk memperbarui pendengar Anda menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih penyeimbang beban dan pilih Pendengar.
4. Pilih Edit pendengar.
5. Untuk Meneruskan ke grup target, pilih grup target.
6. Pilih Simpan.

Untuk memperbarui pendengar Anda menggunakan AWS CLI

Gunakan perintah modifikasi-listener.

Grup sasaran untuk Load Balancer Gateway Anda

Setiap Grup target digunakan untuk merutekan permintaan untuk satu atau lebih target yang terdaftar. Bila Anda membuat pendengar, Anda menentukan grup target untuk tindakan default-nya. Lalu lintas diteruskan ke grup target yang ditentukan dalam aturan pendengar. Anda dapat membuat kelompok-kelompok target yang berbeda untuk berbagai jenis permintaan.

Anda menentukan pengaturan pemeriksaan kesehatan untuk Load Balancer Gateway Anda berdasarkan per grup target. Setiap kelompok target menggunakan pengaturan pemeriksaan kondisi yang sudah ada, kecuali jika Anda menimpa mereka saat Anda membuat kelompok target atau mengubahnya nanti. Setelah Anda menentukan grup target dalam aturan untuk pendengar, Load Balancer Gateway terus memantau kesehatan semua target yang terdaftar dengan grup target yang berada di Availability Zone yang diaktifkan untuk Load Balancer Gateway. Load Balancer Gateway merutekan permintaan ke target terdaftar yang sehat. Untuk informasi selengkapnya, lihat Pemeriksaan kondisi untuk grup target Anda.

Daftar Isi

Konfigurasi perutean

Grup target untuk Gateway Load Balancers mendukung protokol dan port berikut:

- Protokol: GENEVE
- Pelabuhan: 6081

Jenis target

Bila Anda membuat grup target, Anda menentukan jenis target, yang menentukan bagaimana Anda menentukan target. Setelah Anda membuat grup target, Anda tidak dapat mengubah jenis target.

Status yang mungkin muncul adalah sebagai berikut:

`instance`

Target ditentukan oleh instans ID.

`ip`

Target ditentukan oleh alamat IP.

Ketika jenis targetnya adalah `ip`, Anda dapat menentukan alamat IP dari salah satu blok CIDR berikut:

- Subnet dari VPC untuk kelompok target
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

> **Important**
>
> Anda tidak dapat menentukan alamat IP yang dapat dirutekan publik.

Target-target terdaftar.

Load Balancer Gateway Anda berfungsi sebagai titik kontak tunggal untuk klien, dan mendistribusikan lalu lintas masuk ke seluruh target terdaftar yang sehat. Setiap grup target harus

memiliki setidaknya satu target terdaftar di setiap Availability Zone yang diaktifkan untuk Load Balancer Gateway. Anda dapat mendaftarkan setiap target dengan satu atau lebih kelompok target.

Jika permintaan meningkat, Anda dapat mendaftarkan target tambahan dengan satu atau lebih kelompok sasaran untuk menangani permintaan. Load Balancer Gateway mulai merutekan lalu lintas ke target yang baru terdaftar segera setelah proses pendaftaran selesai.

Jika permintaan menurun, atau Anda perlu melayani target Anda, Anda dapat membatalkan pendaftaran target dari kelompok sasaran Anda. Proses deregisterasi target menghapus itu dari kelompok target Anda, tetapi tidak mempengaruhi target sebaliknya. Load Balancer Gateway menghentikan perutean lalu lintas ke target segera setelah dideregistrasi. Target memasuki keadaan `draining` hingga permintaan dalam penerbangan telah selesai. Anda dapat mendaftarkan target dengan grup target lagi ketika Anda siap untuk itu untuk melanjutkan menerima lalu lintas.

Atribut grup target

Anda dapat menggunakan atribut berikut dengan grup target:

`deregistration_delay.timeout_seconds`

Jumlah waktu untuk Elastic Load Balancing menunggu sebelum mengubah keadaan target yang dibatalkan dari `draining` ke `unused`. Rentangnya adalah 0-3600 detik. Nilai default adalah 300 detik.

`stickiness.enabled`

Menunjukkan apakah kelengketan aliran yang dapat dikonfigurasi diaktifkan untuk grup target. Nilai yang mungkin adalah `true` atau `false`. Default-nya adalah salah. Ketika atribut diatur ke`false`, 5_tuple digunakan.

`stickiness.type`

Menunjukkan jenis kelengketan aliran. Nilai yang mungkin untuk grup target yang terkait dengan Gateway Load Balancers adalah:

- `source_ip_dest_ip`
- `source_ip_dest_ip_proto`

`target_failover.on_deregistration`

Menunjukkan bagaimana Load Balancer Gateway menangani alur yang ada saat target dideregistrasi. Nilai yang mungkin adalah `rebalance`

dan `no_rebalance`. Default-nya adalah `no_rebalance`. Kedua atribut (`target_failover.on_deregistrationdantarget_failover.on_unhealthy`) tidak dapat diatur secara independen. Nilai yang Anda tetapkan untuk kedua atribut harus sama.

`target_failover.on_unhealthy`

Menunjukkan bagaimana Load Balancer Gateway menangani alur yang ada saat target tidak sehat. Nilai yang mungkin adalah `rebalance` dan `no_rebalance`. Default-nya adalah `no_rebalance`. Kedua atribut (`target_failover.on_deregistrationdantarget_failover.on_unhealthy`) tidak dapat diatur secara independen. Nilai yang Anda tetapkan untuk kedua atribut harus sama.

Penundaan Pembatalan Pendaftaran

Saat Anda membatalkan pendaftaran target, Load Balancer Gateway mengelola aliran ke target tersebut sebagai berikut:

Arus baru

Load Balancer Gateway berhenti mengirimkan aliran baru.

Arus yang ada

Load Balancer Gateway menangani alur yang ada berdasarkan protokol:

- TCP: Aliran yang ada ditutup jika tidak aktif selama lebih dari 350 detik.
- Protokol lainnya: Arus yang ada ditutup jika tidak aktif selama lebih dari 120 detik.

Untuk membantu menguras aliran yang ada, Anda dapat mengaktifkan penyeimbangan kembali aliran untuk grup target Anda. Untuk informasi selengkapnya, lihat the section called “Kegagalan target”.

Target yang dideregistrasi menunjukkan bahwa itu `draining` sampai batas waktu berakhir. Setelah batas waktu tunda deregistrasi berakhir, target bertransisi ke status. `unused`

Untuk memperbarui nilai penundaan deregistrasi menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Grup Target.

3. Pilih nama grup opsi untuk menampilkan halaman detailnya.
4. Pada halaman Detail grup, pada bagian Atribut, pilih Edit.
5. Pada laman Edit atribut, mengubah nilaiPenundaan Deregistrasiseperlunya.
6. Pilih Simpan perubahan.

Untuk memperbarui nilai penundaan deregistrasi menggunakan AWS CLI

Penggunaan perintah ubah-atribut-grup-target.

Kegagalan target

Dengan failover target, Anda menentukan cara Load Balancer Gateway menangani arus lalu lintas yang ada setelah target menjadi tidak sehat atau ketika target dideregistrasi. Secara default, Load Balancer Gateway terus mengirim aliran yang ada ke target yang sama, bahkan jika target telah gagal atau dideregistrasi. Anda dapat mengelola alur ini dengan mengulangi mereka (`rebalance`) atau membiarkannya di status default (`no_rebalance`).

Tidak ada penyeimbangan kembali:

Load Balancer Gateway terus mengirimkan aliran yang ada ke target yang gagal atau terkuras. Namun, arus baru dikirim ke target yang sehat. Ini adalah perilaku default.

Menyeimbangkan kembali:

Load Balancer Gateway mengulangi alur yang ada dan mengirimkannya ke target sehat setelah batas waktu tunda deregistrasi.

Untuk target yang dideregistrasi, waktu minimum untuk failover akan bergantung pada penundaan deregistrasi. Target tidak ditandai sebagai dideregistrasi sampai penundaan deregistrasi selesai.

Untuk target yang tidak sehat, waktu minimum untuk failover akan tergantung pada konfigurasi pemeriksaan kesehatan kelompok target (ambang waktu interval). Ini adalah waktu minimum sebelum target ditandai sebagai tidak sehat. Setelah waktu ini, Load Balancer Gateway dapat memakan waktu beberapa menit karena waktu propagasi tambahan dan backoff transmisi ulang TCP sebelum mengalihkan aliran baru ke target yang sehat.

Untuk memperbarui nilai failover target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Grup Target.
3. Pilih nama grup opsi untuk menampilkan halaman detailnya.
4. Pada halaman Detail grup, pada bagian Atribut, pilih Edit.
5. Pada halaman Edit atribut, ubah nilai failover Target sesuai kebutuhan.
6. Pilih Simpan perubahan.

Untuk memperbarui nilai failover target menggunakan AWS CLI

Gunakan perintah modify-target-group-attributes, dengan pasangan nilai kunci berikut:

- Kunci = `target_failover.on_deregistration` dan Nilai = `no_rebalance` (default) atau `rebalance`
- Kunci = `target_failover.on_unhealthy` dan Nilai = `no_rebalance` (default) atau `rebalance`

> **Note**
>
> Kedua atribut (`target_failover.on_deregistrationdantarget_failover.on_unhealthy`) harus memiliki nilai yang sama.

Kelengketan aliran

Secara default, Load Balancer Gateway mempertahankan kelengketan aliran ke perangkat target tertentu menggunakan 5-tuple (untuk aliran TCP/UDP). 5-tuple mencakup IP sumber, port sumber, IP tujuan, port tujuan, dan protokol transport. Anda dapat menggunakan atribut stickiness type untuk memodifikasi default (5-tuple) dan memilih 3-tuple (IP sumber, IP tujuan, dan protokol transport) atau 2-tuple (IP sumber dan IP tujuan).

Pertimbangan kelengketan aliran

- Kelengketan aliran dikonfigurasi dan diterapkan pada tingkat grup target, dan ini berlaku untuk semua lalu lintas yang masuk ke grup target.

- Kelengketan aliran 2-tupel dan 3-tupel tidak didukung saat AWS Transit Gateway mode alat dihidupkan. Untuk menggunakan mode alat pada Anda AWS Transit Gateway, gunakan kelengketan aliran 5 tupel pada Load Balancer Gateway Anda
- Kelengketan aliran dapat menyebabkan distribusi koneksi dan aliran yang tidak merata, yang dapat memengaruhi ketersediaan target. Disarankan agar Anda menghentikan atau menguras semua aliran yang ada sebelum memodifikasi tipe lengket dari grup target.

Untuk memperbarui kelengketan aliran menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Grup Target.
3. Pilih nama grup opsi untuk menampilkan halaman detailnya.
4. Pada halaman Detail grup, pada bagian Atribut, pilih Edit.
5. Pada halaman Edit atribut, ubah nilai lengket Flow sesuai kebutuhan.
6. Pilih Simpan perubahan.

Untuk mengaktifkan atau memodifikasi kelengketan aliran menggunakan AWS CLI

Gunakan perintah modify-target-group-attributes dengan atribut dan target group. `stickiness.enabled` `stickiness.type`

Buat grup target untuk Load Balancer Gateway Anda

Anda mendaftarkan target untuk Load Balancer Gateway Anda menggunakan grup target.

Untuk merutekan lalu lintas ke target dalam grup target, membuat pendengar dan menentukan kelompok target dalam tindakan default untuk pendengar. Untuk informasi selengkapnya, lihat Listener.

Anda dapat menambah atau menghapus target dari grup target Anda kapan saja. Untuk informasi selengkapnya, lihat Daftarkan Target-target.. Anda juga dapat mengubah pengaturan pemeriksaan kesehatan untuk grup target Anda. Untuk informasi selengkapnya, lihat Ubah pengaturan pemeriksaan kesehatan.

Untuk membuat grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Pada panel navigasi, di bawah Penyeimbang Beban, pilih Grup Target.
3. Pilih Buat grup target.
4. Konfigurasi dasar
    a. Untuk Pilih jenis target, pilih Instans untuk menentukan target berdasarkan ID instans, atau pilih alamat IP untuk menentukan target berdasarkan alamat IP.
    b. Untuk Name grup traget, masukkan nama untuk grup target. Nama ini harus unik per Wilayah per akun, dapat memiliki maksimum 32 karakter, harus berisi hanya karakter alfanumerik atau tanda hubung, dan tidak harus dimulai atau diakhiri dengan tanda hubung.
    c. Verifikasi bahwa Protokol adalah `GENEVE` dan Port adalah`6081`. Tidak ada protokol atau port lain yang didukung.
    d. Untuk VPC, pilih virtual private cloud (VPC) dengan instance alat keamanan untuk disertakan dalam grup target Anda.
5. (Opsional) Untuk pemeriksaan Kesehatan, ubah pengaturan dan pengaturan lanjutan sesuai kebutuhan. Jika pemeriksaan kesehatan secara berurutan melebihi jumlah Ambang batas tidak sehat, penyeimbang beban mengambil target keluar dari layanan. Jika pemeriksaan kesehatan secara berurutan melebihi jumlah Ambang batas sehat, penyeimbang beban menempatkan target kembali dalam pelayanan. Untuk informasi selengkapnya, lihat Pemeriksaan kondisi untuk grup target Anda.
6. (Opsional) Perluas Tag dan tambahkan tag yang Anda butuhkan.
7. Pilih Selanjutnya.
8. Untuk Register target tambahkan satu atau beberapa target sebagai berikut:
    - Jika jenis target adalahInstansPilih satu atau beberapa instans, masukkan satu atau beberapa port, lalu pilihSertakan sebagai tertunda di bawah ini.
    - Jika jenis target Alamat IP, pilih rangkaian, masukkan alamat IP dan port, dan kemudian pilih Sertakan sebagai tertunda di bawah ini.
9. Pilih Buat grup target.

Untuk membuat grup target menggunakan AWS CLI

Penggunaan perintahmembuat-target-kelompok untuk membuat grup target,Penambahan tagperintah untuk menandai kelompok target Anda, dan perintahRegister-targetuntuk menambahkan target.

Pemeriksaan kondisi untuk grup target Anda

Anda mendaftarkan target Anda dengan satu atau lebih grup target. Load Balancer Gateway Anda mulai merutekan permintaan ke target yang baru terdaftar segera setelah proses pendaftaran selesai. Diperlukan waktu beberapa menit agar proses pendaftaran selesai dan untuk memulai pemeriksaan kesehatan.

Load Balancer Gateway secara berkala mengirimkan permintaan ke setiap target yang terdaftar untuk memeriksa statusnya. Setelah setiap pemeriksaan kesehatan selesai, Load Balancer Gateway menutup koneksi yang dibuat untuk pemeriksaan kesehatan.

Pengaturan pemeriksaan kondisi

Anda mengonfigurasi pemeriksaan kesehatan aktif untuk target dalam grup target dengan menggunakan pengaturan berikut. Jika pemeriksaan kesehatan melebihi jumlah kegagalan UnhealthyThresholdCountberturut-turut yang ditentukan, Load Balancer Gateway menghilangkan target dari layanan. Ketika pemeriksaan kesehatan melebihi jumlah keberhasilan HealthyThresholdCountberturut-turut yang ditentukan, Load Balancer Gateway menempatkan target kembali dalam layanan.

Pengaturan	Deskripsi
HealthCheckProtocol	Protokol yang digunakan penyeimbang beban saat melakukan pemeriksaan kesehatan pada target. Protokol yang mungkin adalah HTTP, HTTPS, dan TCP. Defaultnya adalah TCP.
HealthCheckPort	Port yang digunakan Gateway Load Balancer saat melakukan pemeriksaan kesehatan pada target. Kisarannya adalah 1 hingga 65535. Defaultnya adalah 80.
HealthCheckPath	[Pemeriksaan kesehatan HTTP/HTTPS] Jalur pemeriksaan kesehatan yang menjadi tujuan pada target pemeriksaan kesehatan. Default-n ya adalah /.
HealthCheckTimeoutSeconds	Jumlah waktu, dalam detik, selama tidak ada respons dari target berarti pemeriksaan

Pengaturan	Deskripsi
	kondisi gagal. Kisarannya adalah 2 hingga 120. Default-nya adalah 5.
HealthCheckIntervalSeconds	Perkiraan jumlah waktu, dalam detik, antara pemeriksaan kondisi dari target individu. Kisarannya adalah 5 hingga 300. Defaultny a adalah 10 detik. Nilai ini harus lebih besar dari atau sama dengan HealthCheckTimeout Seconds. **Important** Pemeriksaan Kesehatan untuk Gateway Load Balancer didistrib usikan dan menggunakan mekanisme konsensus untuk menentukan kesehatan target. Oleh karena itu, Anda harus mengharapkan peralatan target menerima beberapa pemeriksaan kesehatan dalam interval waktu yang dikonfigurasi.
HealthyThresholdCount	Jumlah pemeriksaan kesehatan yang berhasil berturut-turut diperlukan sebelum mempertim bangkan kesehatan target yang tidak sehat. Rentangnya adalah 2 hingga 10. Default-nya adalah 5.
UnhealthyThresholdCount	Jumlah pemeriksaan kondisi yang gagal berturut-turut diperlukan sebelum mengangga p target yang tidak memiliki kondisi sehat. Rentangnya adalah 2 hingga 10. Defaultnya adalah 2.

Pengaturan	Deskripsi
Matcher	[Pemeriksaan kesehatan HTTP/HTTPS] Kode HTTP yang digunakan saat memeriksa respons yang berhasil dari target. Nilai ini harus 200-399.

Status kondisi target

Sebelum Load Balancer Gateway mengirimkan permintaan pemeriksaan kesehatan ke target, Anda harus mendaftarkannya ke grup target, menentukan grup targetnya dalam aturan listener, dan memastikan bahwa Availability Zone target diaktifkan untuk Load Balancer Gateway.

Tabel berikut menjelaskan nilai yang mungkin untuk status kondisi target terdaftar.

Nilai	Deskripsi
`initial`	Load Balancer Gateway sedang dalam proses mendaftar kan target atau melakukan pemeriksaan kesehatan awal pada target. Kode alasan terkait: `Elb.RegistrationIn Progress` | `Elb.InitialHealthChecking`
`healthy`	Targetnya sehat. Kode alasan terkait: Tidak ada
`unhealthy`	Target tidak merespon pemeriksaan kesehatan atau gagal pemeriksaan kesehatan. Kode alasan terkait: `Target.FailedHealthChecks`
`unused`	Target tidak terdaftar dengan grup target, grup target tidak digunakan dalam aturan pendengar, target ada di Availability Zone yang tidak diaktifkan, atau target dalam keadaan berhenti atau dihentikan.

Nilai	Deskripsi
	Kode alasan terkait: `Target.NotRegistered | Target.NotInUse | Target.InvalidState | Target.IpUnusable`
`draining`	Target membatalkan pendaftaran dan pengosongan koneksi sedang dalam proses. Kode alasan terkait: `Target.DeregistrationInProgress`
`unavailable`	Target kesehatan tidak tersedia. Kode alasan terkait: `Elb.InternalError`

Kode alasan pemeriksaan kondisi

Jika status target adalah nilai apa pun selain`Healthy`, API mengembalikan kode alasan dan deskripsi masalah, dan konsol menampilkan deskripsi yang sama. Kode alasan yang dimulai dengan `Elb` berasal dari sisi Load Balancer Gateway dan kode alasan yang dimulai `Target` dengan berasal dari sisi target.

Kode alasan	Deskripsi
`Elb.InitialHealthChecking`	Pemeriksaan kondisi awal sedang berlangsung
`Elb.InternalError`	Pemeriksaan kondisi gagal karena kesalahan internal
`Elb.RegistrationInProgress`	Pendaftaran target sedang berlangsung
`Target.DeregistrationInProgress`	Pembatalan pendaftaran target sedang berlangsung
`Target.FailedHealthChecks`	Pemeriksaan kesehatan gagal
`Target.InvalidState`	Target berada dalam keadaan berhenti

Kode alasan	Deskripsi
	Target dalam keadaan dihentikan Target berada dalam keadaan dihentikan atau berhenti Target dalam keadaan tidak valid
`Target.IpUnusable`	Alamat IP tidak dapat digunakan sebagai target, karena digunakan oleh penyeimbang beban
`Target.NotInUse`	Grup target tidak dikonfigurasi untuk menerima lalu lintas dari Load Balancer Gateway Target berada di Availability Zone yang tidak diaktifkan untuk Load Balancer Gateway
`Target.NotRegistered`	Target tidak terdaftar ke grup target

Skenario kegagalan target Load Balancer Gateway

Alur yang ada: Secara default, arus yang ada pergi ke target yang sama kecuali waktu aliran habis atau diatur ulang, terlepas dari kesehatan dan status registrasi target. Pendekatan ini memfasilitasi pengeringan koneksi, dan mengakomodasi firewall pihak ketiga yang terkadang tidak dapat menanggapi pemeriksaan kesehatan karena penggunaan CPU yang tinggi. Untuk informasi selengkapnya, lihat Target failover.

Arus baru: Arus baru dikirim ke target yang sehat. Ketika keputusan load balancing untuk aliran telah dibuat, Load Balancer Gateway akan mengirim aliran ke target yang sama bahkan jika target tersebut menjadi tidak sehat, atau target lain menjadi sehat.

Ketika semua target tidak sehat, Load Balancer Gateway memilih target secara acak dan meneruskan lalu lintas ke sana selama masa pakai arus, hingga disetel ulang atau habis waktunya. Karena lalu lintas diteruskan ke target yang tidak sehat, lalu lintas dijatuhkan sampai target itu menjadi sehat kembali.

TLS 1.3: Jika grup target dikonfigurasi dengan pemeriksaan kesehatan HTTPS, target terdaftarnya gagal dalam pemeriksaan kesehatan jika mereka hanya mendukung TLS 1.3. Target ini harus mendukung versi TLS sebelumnya, seperti TLS 1.2.

Penyeimbangan beban lintas zona: Secara default, penyeimbangan beban di seluruh Availability Zone dinonaktifkan. Jika load balancing di seluruh zona diaktifkan, setiap Load Balancer Gateway dapat melihat semua target di semua Availability Zone, dan semuanya diperlakukan sama, terlepas dari zonanya.

Keputusan penyeimbangan beban dan pemeriksaan kesehatan selalu independen di antara zona. Bahkan ketika penyeimbangan beban di seluruh zona diaktifkan, perilaku untuk aliran yang ada dan aliran baru sama seperti yang dijelaskan di atas. Untuk informasi lebih lanjut, lihat Penyeimbang beban lintas zona di Panduan Pengguna Elastic Load Balancing.

Periksa kondisi target Anda

Anda dapat memeriksa status kondisi target yang terdaftar dengan kelompok target Anda.

Untuk memeriksa kesehatan target Anda menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbang Beban, pilih Grup Target.
3. Pilih nama target grup untuk menampilkan halaman detailnya.
4. Pada tab Target, kolom Status menunjukkan status setiap target.
5. Jika status target adalah nilai selain `Healthy`, kolom Rincian status berisi informasi lebih lanjut.

Untuk memeriksa kesehatan target Anda menggunakan AWS CLI

Gunakan perintah describe-target-health. Keluaran dari perintah ini berisi status kesehatan target. Ini termasuk kode alasan jika statusnya adalah nilai selain `Healthy`.

Untuk menerima pemberitahuan email tentang target yang tidak sehat

Gunakan CloudWatch alarm untuk memicu fungsi Lambda untuk mengirim detail tentang target yang tidak sehat. Untuk step-by-step petunjuk, lihat posting blog berikut: Mengidentifikasi target penyeimbang beban Anda yang tidak sehat.

Ubah pengaturan pemeriksaan kesehatan

Anda dapat mengubah beberapa pengaturan pemeriksaan kesehatan untuk grup target Anda.

Untuk mengubah pengaturan pemeriksaan kesehatan untuk grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Pada panel navigasi, di bawah Penyeimbang Beban, pilih Grup Target.
3. Pilih nama target grup untuk menampilkan halaman detailnya.
4. Pada tab Detail grup, di bagian Pengaturan pemeriksaan kondisi, pilih Edit.
5. Pada halaman Mengedit pengaturan pemeriksaan kondisi, ubah pengaturan sesuai kebutuhan, lalu pilih Simpan perubahan.

Untuk mengubah pengaturan pemeriksaan kesehatan untuk grup target menggunakan AWS CLI

Gunakan perintah modify-target-group.

Daftarkan target dengan grup target Anda

Ketika target Anda siap untuk menangani permintaan, Anda mendaftarkannya dengan satu atau lebih kelompok target. Anda dapat mendaftarkan target dengan instans ID atau dengan alamat IP. Load Balancer Gateway mulai merutekan permintaan ke target segera setelah proses pendaftaran selesai dan target melewati pemeriksaan kesehatan awal. Diperlukan waktu beberapa menit hingga proses pendaftaran selesai dan pemeriksaan kondisi dimulai. Untuk informasi selengkapnya, lihat Pemeriksaan kondisi untuk grup target Anda.

Jika permintaan pada target Anda yang saat ini terdaftar meningkat, Anda dapat mendaftarkan target tambahan untuk menangani permintaan. Jika permintaan pada target Anda yang terdaftar menurun, Anda dapat membatalkan pendaftaran target dari grup target Anda. Diperlukan beberapa menit agar proses deregistrasi selesai dan agar Load Balancer Gateway menghentikan permintaan perutean ke target. Jika permintaan meningkat kemudian, Anda dapat mendaftarkan target yang Anda batalkan pendaftarannya dengan grup target lagi. Jika Anda perlu melayani target, Anda dapat membatalkan pendaftaran dan kemudian mendaftar lagi ketika servis selesai.

Ketika Anda membatalkan pendaftaran target, Elastic Load Balancing menunggu hingga permintaan dalam penerbangan selesai. Hal ini dikenal sebagai Pengosongan koneksi. Status target adalah `draining` sementara pengosongan koneksi sedang berlangsung. Setelah deregistrasi selesai, status target berubah ke `unused`. Untuk informasi selengkapnya, lihat Penundaan Pembatalan Pendaftaran.

Menargetkan grup keamanan

Ketika Anda mendaftarkan instans EC2 sebagai target, Anda harus memastikan bahwa grup keamanan untuk instans ini memungkinkan lalu lintas masuk dan keluar pada port 6081.

Gateway Load Balancer tidak memiliki grup keamanan terkait. Oleh karena itu, grup keamanan untuk target Anda harus menggunakan alamat IP untuk memungkinkan lalu lintas dari penyeimbang beban.

ACL jaringan

Ketika Anda mendaftarkan instans EC2 sebagai target, Anda harus memastikan bahwa daftar kontrol akses jaringan (ACL) untuk subnet untuk instans Anda memungkinkan lalu lintas pada port 6081. ACL jaringan default untuk VPC memungkinkan semua lalu lintas masuk dan keluar. Jika Anda membuat ACL jaringan kustom, verifikasi bahwa mereka mengizinkan lalu lintas yang sesuai.

Mendaftar atau membatalkan pendaftaran target

Setiap grup target harus memiliki setidaknya satu target terdaftar di setiap Availability Zone yang diaktifkan untuk Load Balancer Gateway.

Jenis target grup target Anda menentukan bagaimana Anda mendaftarkan target dengan kelompok target tersebut. Untuk informasi selengkapnya, lihat Jenis target.

Persyaratan

- Anda tidak dapat mendaftarkan target di seluruh peering VPC Antar wilayah.
- Anda tidak dapat mendaftarkan instance berdasarkan ID instans di seluruh peering VPC intra-wilayah, tetapi Anda dapat mendaftarkannya berdasarkan alamat IP.

Daftar Isi

Mendaftarkan atau membatalkan pendaftaran target berdasarkan ID instans

Suatu instans harus berada di negara `running` saat Anda mendaftarkannya.

Untuk mendaftarkan atau membatalkan pendaftaran target berdasarkan ID instans menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Grup Target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pilih tabTarget.
5. Untuk mendaftarkan contoh, pilihTarget daftar. Pilih satu atau beberapa contoh, lalu pilih Sertakan sebagai tertunda di bawah ini. Setelah selesai menambahkan instans, pilih Daftarkan target tertunda.
6. Untuk membatalkan pendaftaran instans, pilih instans, lalu pilih Deregister.

Mendaftarkan atau membatalkan pendaftaran target berdasarkan alamat IP

Alamat IP yang Anda daftarkan harus dari salah satu blok CIDR berikut:

- Subnet dari VPC untuk grup target
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Untuk mendaftarkan atau membatalkan pendaftaran target berdasarkan alamat IP menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Grup Target.
3. Pilih nama grup target untuk membuka halaman perinciannya.
4. Pilih tabTarget.
5. Untuk mendaftarkan alamat IP, pilih Daftarkan target. Untuk setiap alamat IP, pilih jaringan, Availability Zone, alamat IP, dan port, dan kemudian pilih sertakan sebagai tertunda di bawah. Setelah selesai menentukan alamat, pilih Daftarkan target tertunda.
6. Untuk membatalkan pendaftaran alamat IP, pilih alamat IP, lalu pilihDeregister. Jika Anda memiliki banyak alamat IP terdaftar, menambahkan filter atau mengubah urutan pengurutan mungkin akan membantu Anda.

Mendaftar atau membatalkan pendaftaran target menggunakan AWS CLI

Gunakan perintah daftar-targetuntuk menambahkan target dan perintah mendaftarkan ulang-target untuk menghapus target.

Tag untuk grup target

Tag membantu Anda mengategorikan grup target Auto dengan berbagai cara, misalnya, berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap grup Auto Scaling. Tombol tag harus unik untuk setiap kelompok target. Jika Anda menambahkan tag dengan kunci yang sudah terkait dengan grup target, maka akan memperbarui nilai tag tersebut.

Setelah selesai dengan tag, Anda dapat menghapusnya.

Pembatasan

- Jumlah maksimum tanda per sumber daya—50
- Panjang kunci maksimum – 127 karakter Unicode
- Panjang nilai maksimum—255 karakter Unicode
- Kunci dan nilai tag peka huruf besar/kecil. Karakter yang diizinkan adalah huruf, spasi, dan angka yang dapat diwakili dalam UTF-8, ditambah karakter khusus berikut: + - = . _:/@. Jangan gunakan spasi terkemuka atau paling belakang.
- Jangan gunakan `aws:` awalan dalam nama atau nilai tag Anda karena itu dicadangkan untuk AWS digunakan. Anda tidak dapat mengedit atau menghapus nama atau nilai tag dengan awalan ini. Tag dengan awalan ini tidak dihitung terhadap tag Anda per batas sumber daya.

Untuk memperbarui tag untuk grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Grup Target.
3. Pilih nama grup opsi untuk menampilkan halaman detailnya.
4. Pada tab Tag, pilih Kelola tag dan lakukan satu atau beberapa hal berikut:
    a. Untuk memperbarui tag, masukkan nilai baru untukKuncidanNilai.
    b. Untuk menambahkan tag, pilih Tambahkan Tag dan masukkan nilai untuk Kunci dan Nilai

c. Untuk menghapus sebuah tag, pilih Remove di samping tag yang akan dihapus.

5. Setelah selesai memperbarui tag, pilihSimpan perubahan.

Untuk memperbarui tag untuk grup target menggunakan AWS CLI

Penggunaan perintahPenambahan tagdanHapus tag.

Menghapus grup target

Anda dapat menghapus kelompok target jika tidak direferensikan oleh tindakan lanjut dari aturan pendengar. Menghapus kelompok target tidak mempengaruhi target terdaftar dengan kelompok target. Jika Anda tidak lagi membutuhkan instance EC2 terdaftar, Anda dapat menghentikan atau menghapusnya.

Untuk menghapus grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbang Beban, pilih Grup Target.
3. Pilih grup target dan pilih Tindakan, Hapus.
4. Saat diminta konfirmasi, pilih Ya, hapus.

Untuk menghapus grup target menggunakan AWS CLI

Gunakan perintah hapus target grup .

Pantau Load Balancer Gateway Anda

Anda dapat menggunakan fitur berikut untuk memantau Load Balancer Gateway Anda untuk menganalisis pola lalu lintas, dan untuk memecahkan masalah. Namun, Load Balancer Gateway tidak menghasilkan log akses karena merupakan penyeimbang beban lapisan 3 transparan yang tidak menghentikan aliran. Untuk menerima log akses, Anda harus mengaktifkan pencatatan akses pada peralatan target Load Balancer Gateway seperti firewall, IDS/IPS, dan peralatan keamanan. Selain itu, Anda juga dapat memilih untuk mengaktifkan log aliran VPC di Gateway Load Balancers.

CloudWatch metrik

Anda dapat menggunakan Amazon CloudWatch untuk mengambil statistik tentang titik data untuk Gateway Load Balancers dan target sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anda dapat menggunakan metrik ini untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Untuk informasi selengkapnya, lihat CloudWatch metrik untuk Load Balancer Gateway Anda.

Log Aliran VPC

Anda dapat menggunakan VPC Flow Logs untuk menangkap informasi terperinci tentang lalu lintas yang menuju dan dari Load Balancer Gateway Anda. Untuk informasi selengkapnya, lihat Log aliran VPC di Panduan Pengguna Amazon VPC.

Buat log alur untuk setiap antarmuka jaringan untuk Load Balancer Gateway Anda. Ada satu antarmuka jaringan per subnet. Untuk mengidentifikasi antarmuka jaringan untuk Load Balancer Gateway, cari nama Gateway Load Balancer di bidang deskripsi antarmuka jaringan.

Ada dua entri untuk setiap koneksi melalui Load Balancer Gateway Anda, satu untuk koneksi frontend antara klien dan Load Balancer Gateway, dan yang lainnya untuk koneksi backend antara Load Balancer Gateway dan target. Jika target terdaftar oleh ID instans, sambungan muncul ke instans sebagai sambungan dari klien. Jika grup keamanan instance tidak mengizinkan koneksi dari klien tetapi ACL jaringan untuk subnet mengizinkannya, log untuk antarmuka jaringan untuk Load Balancer Gateway menunjukkan “TERIMA OK” untuk koneksi frontend dan backend, sedangkan log untuk antarmuka jaringan untuk instance menunjukkan “TOLAK OK” untuk koneksi.

CloudTrail log

Anda dapat menggunakan AWS CloudTrail untuk menangkap informasi terperinci tentang panggilan yang dilakukan ke Elastic Load Balancing API, dan menyimpannya sebagai file log

di Amazon S3. Anda dapat menggunakan CloudTrail log ini untuk menentukan panggilan mana yang dilakukan, alamat IP sumber dari mana panggilan itu berasal, siapa yang melakukan panggilan, kapan panggilan dilakukan, dan sebagainya. Untuk informasi selengkapnya, lihat Logging API call untuk Load Balancer Gateway Anda menggunakan AWS CloudTrail.

CloudWatch metrik untuk Load Balancer Gateway Anda

Elastic Load Balancing menerbitkan titik data ke Amazon CloudWatch untuk Load Balancer Gateway dan target Anda. CloudWatch memungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anggap metrik sebagai variabel untuk memantau, dan titik data sebagai nilai variabel tersebut dari waktu ke waktu. Misalnya, Anda dapat memantau jumlah total target sehat untuk Load Balancer Gateway selama periode waktu tertentu. Setiap titik data memiliki stempel waktu terkait dan unit pengukuran opsional.

Anda dapat menggunakan metrik untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Misalnya, Anda dapat membuat CloudWatch alarm untuk memantau metrik tertentu dan memulai tindakan (seperti mengirim pemberitahuan ke alamat email) jika metrik berada di luar rentang yang Anda anggap dapat diterima.

Elastic Load Balancing melaporkan metrik CloudWatch hanya jika permintaan mengalir melalui Load Balancer Gateway. Jika ada permintaan yang mengalir, Elastic Load Balancing mengukur dan mengirimkan metriknya dalam interval 60 detik. Jika tidak ada permintaan yang mengalir atau tidak ada data untuk metrik, metrik tidak dilaporkan.

Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

Metrik Load Balancer Gateway

Namespace `AWS/GatewayELB` mencakup metrik berikut.

Metrik	Deskripsi
`ActiveFlowCount`	Jumlah total arus bersamaan (atau koneksi) dari klien ke target. Kriteria pelaporan: Ada nilai bukan nol Statistik: Statistik yang paling berguna adalah `Average`, `Maximum`, dan `Minimum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ConsumedLCUs`	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda. Anda membayar untuk jumlah LCU yang digunakan per jam. Untuk informasi lebih lanjut, lihat Harga Elastic Load Balancing. Reporting criteria: Selalu dilaporkan Statistics: Semua Dimensi • `LoadBalancer`
`HealthyHostCount`	Jumlah target yang dianggap sehat. Reporting criteria: Dilaporkan jika pemeriksaan kondisi diaktifkan Statistik: Statistik yang paling berguna adalah `Maximum` dan `Minimum`. Dimensi • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`NewFlowCount`	Jumlah total arus baru (atau koneksi) didirikan dari klien ke target dalam periode waktu.

Metrik	Deskripsi
	Reporting criteria: Ada nilai bukan nol Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes`	Jumlah total byte yang diproses oleh penyeimbang beban. Jumlah ini termasuk lalu lintas ke dan dari target, tetapi bukan lalu lintas pemeriksaan kesehatan. Reporting criteria: Ada nilai bukan nol Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`UnHealthyHostCount`	Jumlah target yang dianggap tidak sehat. Reporting criteria: Dilaporkan jika pemeriksaan kondisi diaktifkan Statistik: Statistik yang paling berguna adalah `Maximum` dan `Minimum`. Dimensi • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Dimensi metrik untuk Gateway Load Balancers

Untuk memfilter metrik untuk Load Balancer Gateway Anda, gunakan dimensi berikut.

Dimensi	Deskripsi
`AvailabilityZone`	Memfilter data metrik berdasarkan Availability Zone.
`LoadBalancer`	Memfilter data metrik dengan Gateway Load Balancer. Tentukan Load Balancer Gateway sebagai berikut: gateway/ load-balancer-name /1234567890123456 (bagian akhir dari ARN).
`TargetGroup`	Memfilter data metrik berdasarkan grup target. Tentukan kelompok target sebagai berikut: targetgroup/ target-group-name/1234567890123456 (bagian akhir dari kelompok target ARN).

Lihat CloudWatch metrik untuk Load Balancer Gateway

Anda dapat melihat CloudWatch metrik untuk Gateway Load Balancers menggunakan konsol Amazon EC2. Metrik ini ditampilkan sebagai grafik pemantauan. Grafik pemantauan menunjukkan titik data jika Load Balancer Gateway aktif dan menerima permintaan.

Atau, Anda dapat melihat metrik untuk Load Balancer Gateway menggunakan CloudWatch konsol.

Untuk melihat metrik menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Untuk melihat metrik yang difilter oleh grup target, lakukan hal berikut:
   a. Di panel navigasi, pilih Grup Keamanan.
   b. Pilih grup target Anda dan pilih Pemantauan.
   c. (Opsional) Untuk memfilter hasil berdasarkan waktu, pilih rentang waktu dari Menampilkan data untuk.
   d. Untuk mendapatkan tampilan yang lebih besar dari satu metrik, pilih grafiknya.
3. Untuk melihat metrik yang difilter oleh Load Balancer Gateway, lakukan hal berikut:
   a. Di panel navigasi, pilih Load Balancers.
   b. Pilih Load Balancer Gateway Anda dan pilih Monitoring.
   c. (Opsional) Untuk memfilter hasil berdasarkan waktu, pilih rentang waktu dari Showing data for.

d. Untuk mendapatkan tampilan yang lebih besar dari satu metrik, pilih grafiknya.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih namespace GatewayelB.
4. (Opsional) Untuk melihat metrik di semua dimensi, masukkan namanya di kolom pencarian.

Untuk melihat metrik menggunakan AWS CLI

Gunakan perintah list-metrics berikut untuk mencantumkan metrik yang tersedia:

```
aws cloudwatch list-metrics --namespace AWS/GatewayELB
```

Untuk mendapatkan statistik untuk metrik menggunakan AWS CLI

Gunakan get-metric-statisticsperintah berikut dapatkan statistik untuk metrik dan dimensi yang ditentukan. Perhatikan bahwa CloudWatch memperlakukan setiap kombinasi dimensi yang unik sebagai metrik terpisah. Anda tidak dapat mengambil statistik menggunakan kombinasi dimensi yang diterbitkan secara khusus. Anda harus menentukan dimensi yang sama yang digunakan saat metrik dibuat.

```
aws cloudwatch get-metric-statistics --namespace AWS/GatewayELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

Berikut ini adalah output contoh.

```
{
    "Datapoints": [
        {
            "Timestamp": "2020-12-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
```

```
        {
            "Timestamp": "2020-12-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Logging API call untuk Load Balancer Gateway Anda menggunakan AWS CloudTrail

Elastic Load Balancing terintegrasi dengan AWS CloudTrail layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan dalam Elastic Load Balancing. CloudTrail menangkap semua panggilan API untuk Elastic Load Balancing sebagai peristiwa. Panggilan yang diambil mencakup panggilan dari panggilan AWS Management Console dan kode ke operasi Elastic Load Balancing API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Elastic Load Balancing. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Elastic Load Balancing, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Elastic Load Balancing di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Elastic Load Balancing, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Elastic Load Balancing, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file

log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua tindakan Elastic Load Balancing untuk Gateway Load Balancer dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Elastic Load Balancing versi 2015-12-01. Misalnya, panggilan ke `CreateLoadBalancer` dan `DeleteLoadBalancer` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Baik permintaan tersebut dibuat dengan kredensial pengguna atau root.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat elemen CloudTrailUserIdentity.

Memahami entri berkas log Elastic Load Balancing

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa merepresentasikan satu permintaan dari sumber apa pun dan menyertakan informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

File log menyertakan peristiwa untuk semua panggilan AWS API untuk AWS akun Anda, bukan hanya panggilan Elastic Load Balancing API. Anda dapat menemukan panggilan ke API Elastic Load Balancing dengan memeriksa elemen `eventSource` dengan nilai

`elasticloadbalancing.amazonaws.com`. Untuk melihat catatan tindakan tertentu, seperti `CreateLoadBalancer`, periksa elemen `eventName` dengan nama tindakan.

Berikut ini adalah contoh catatan CloudTrail log untuk Elastic Load Balancing untuk pengguna yang membuat Load Balancer Gateway dan kemudian menghapusnya menggunakan. AWS CLI Anda dapat mengidentifikasi CLI menggunakan elemen `userAgent`. Anda dapat mengidentifikasi panggilan API yang diminta menggunakan elemen `eventName`. Informasi tentang pengguna (`Alice`) dapat ditemukan di elemen `userIdentity`.

Example Contoh: CreateLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2020-12-11T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "name": "my-load-balancer",
        "type": "gateway"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "gateway",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "createdTime": "Dec 11, 2020 5:23:50 PM",
```

```
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0",
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example Contoh: DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2020-12-12T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Kuota untuk Penyeimbang Beban Gateway Anda

Akun AWS Anda memiliki kuota default, yang sebelumnya disebut sebagai batas, untuk setiap layanan AWS. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk meminta penambahan kuota, gunakan formulir kenaikan batas

Penyeimbang beban

AWSAkun Anda memiliki kuota berikut yang terkait dengan Penyeimbang Beban Gateway.

Nama	Default	Dapat Disesuaikan
Gateway Load Balancer per Wilayah	100	Ya
Gateway Load Balancer per VPC	100	Ya
Gateway Load Balancer per VPC	300*	Ya
Pendengar untuk Load Balancer Gateway	1	Tidak

* Setiap Gateway Load Balancer menggunakan satu antarmuka jaringan per zona.

Kelompok-kelompok target

Kuota berikut adalah untuk grup target.

Nama	Default	Dapat Disesuaikan
Grup target GENEVE per Wilayah	100	Ya
Target per grup target	1.000	Ya
Target per Availability Zone per grup target GENEVE	300	Tidak
Target per Availability Zone per Load Balancer Gateway	300	Tidak

Nama	Default	Dapat Disesuaikan
Target per Load Balancer Gateway	300	Tidak

Bandwidth

Secara default, setiap endpoint VPC dapat mendukung bandwidth hingga 10 Gbps per Availability Zone dan secara otomatis menskalakan hingga 100 Gbps. Jika aplikasi Anda membutuhkan throughput yang lebih tinggi, hubungiAWS dukungan.

Riwayat dokumen untuk Gateway Load Balancers

Tabel berikut menjelaskan rilis untuk Gateway Load Balancers.

Perubahan	Deskripsi	Tanggal
Dukungan IPv6	Anda dapat mengonfigurasi Load Balancer Gateway Anda untuk mendukung alamat IPv4 dan IPv6.	12 Desember 2022
Penyeimbangan kembali aliran	Rilis ini menambahkan dukungan untuk menentuka n perilaku penanganan aliran untuk Gateway Load Balancers ketika target gagal atau deregister.	13 Oktober 2022
Kelengketan aliran yang dapat dikonfigurasi	Anda dapat mengonfigurasi hashing yang mempertah ankan kelengketan aliran ke alat target tertentu.	Agustus 25, 2022
Tersedia di wilayah baru	Rilis ini menambahkan dukungan untuk Gateway Load Balancers di wilayah. AWS GovCloud (US)	17 Juni 2021
Tersedia di wilayah baru	Rilis ini menambahkan dukungan untuk Gateway Load Balancers di wilayah Kanada (Tengah), Asia Pasifik (Seoul), dan Asia Pasifik (Osaka).	31 Maret 2021
Tersedia di wilayah baru	Rilis ini menambahkan dukungan untuk Gateway Load Balancers di AS	19 Maret 2021

	Barat (California N.), Eropa (London), Eropa (Paris), Eropa (Milan), Afrika (Cape Town), Timur Tengah (Bahrain), Asia Pasifik (Hong Kong), Asia Pasifik (Singapura), dan Asia Pasifik (Mumbai).	
Rilis awal	Rilis Elastic Load Balancing ini memperkenalkan Gateway Load Balancer.	10 November 2020

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.