Penyeimbang Beban Jaringan

Elastic Load Balancing

Elastic Load Balancing: Penyeimbang Beban Jaringan

Table of Contents

Apa itu Penyeimbang Beban Jaringan?

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas masuk Anda ke beberapa target, seperti instans EC2, kontainer, dan alamat IP, 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 penyeimbang beban yang paling sesuai dengan kebutuhan Anda. Panduan ini membahas Penyeimbang Beban Jaringan. Untuk informasi selengkapnya tentang penyeimbang beban lainnya, lihat Panduan pengguna untuk Application Load Balancer, Panduan pengguna untuk Gateway Load Balancer, dan Panduan pengguna untuk Classic Load Balancer.

Komponen Penyeimbang Beban Jaringan

Sebuah penyeimbang beban berfungsi sebagai titik kontak tunggal untuk klien. Penyeimbang beban mendistribusikan lalu lintas masuk di beberapa target, seperti instans Amazon EC2. Hal ini akan meningkatkan ketersediaan aplikasi Anda. Anda menambahkan satu atau lebih pendengar ke penyeimbang beban Anda.

Pendengar memeriksa permintaan koneksi dari klien, menggunakan protokol dan port yang Anda mengkonfigurasi, dan meneruskan permintaan ke grup target.

Grup target merutekan permintaan ke satu atau beberapa target terdaftar, seperti instans EC2, menggunakan protokol dan nomor port yang Anda tentukan. Grup target Network Load Balancer mendukung protokol TCP, UDP, TCP_UDP, dan TLS. Anda dapat mendaftarkan target dengan beberapa grup target. Anda dapat mengonfigurasi pemeriksaan kondisi berdasarkan per grup target. Pemeriksaan kesehatan dilakukan pada semua target yang terdaftar ke grup target yang ditentukan dalam aturan pendengar untuk penyeimbang beban Anda.

Untuk informasi lebih lanjut, lihat dokumentasi berikut ini:

- Penyeimbang beban
- Pendengar
- Kelompok sasaran

Gambaran umum Penyeimbang Beban Jaringan

Penyeimbang Beban jaringan berfungsi pada lapisan keempat dari model Open Systems Interkoneksi (OSI). Hal ini dapat menangani jutaan permintaan per detik. Setelah penyeimbang beban menerima permintaan koneksi, ia memilih target dari grup target untuk aturan default. Ia mencoba untuk membuka koneksi TCP ke target yang dipilih pada port yang ditentukan dalam konfigurasi pendengar.

Saat Anda mengaktifkan Availability Zone untuk penyeimbang beban, Elastic Load Balancing menciptakan simpul penyeimbang beban di Availability Zone. 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 simpul penyeimbang beban mendistribusikan lalu lintas di seluruh target yang terdaftar di semua Availability Zone yang diaktifkan. Untuk informasi selengkapnya, lihat Zona Ketersediaan.

Untuk meningkatkan toleransi kesalahan aplikasi Anda, Anda dapat mengaktifkan beberapa Availability Zone untuk penyeimbang beban Anda dan memastikan bahwa setiap grup target memiliki setidaknya satu target di setiap Availability Zone yang diaktifkan. Sebagai contoh, jika satu atau lebih kelompok target tidak memiliki target yang sehat di Availability Zone, kami menghapus alamat IP untuk subnet yang sesuai dari DNS, tetapi simpul penyeimbang beban di Availability Zone lain masih tersedia untuk rute lalu lintas. Jika klien tidak menghormati time-to-live (TTL) dan mengirim permintaan ke alamat IP setelah dihapus dari DNS, permintaan gagal.

Untuk lalu lintas TCP, penyeimbang beban memilih target menggunakan algoritma hash aliran berdasarkan protokol, alamat IP sumber, port sumber, alamat IP tujuan, port tujuan, dan nomor urutan TCP. Sambungan TCP dari klien memiliki port sumber yang berbeda dan nomor urut, dan dapat diarahkan ke target yang berbeda. Setiap sambungan TCP individu diarahkan ke satu target untuk kehidupan sambungan.

Untuk lalu lintas UDP, penyeimbang beban memilih target menggunakan algoritma hash aliran berdasarkan protokol, alamat IP sumber, port sumber, alamat IP tujuan, dan port tujuan. Aliran UDP memiliki sumber dan tujuan yang sama, sehingga secara konsisten diarahkan ke target tunggal sepanjang masa pakainya. Aliran UDP yang berbeda memiliki alamat IP sumber yang berbeda dan port, sehingga mereka dapat diarahkan ke target yang berbeda.

Elastic Load Balancing menciptakan antarmuka jaringan untuk setiap Availability Zone yang Anda aktifkan. Setiap simpul penyeimbang beban di Availability Zone menggunakan antarmuka jaringan ini untuk mendapatkan alamat IP statis. Bila Anda membuat penyeimbang beban menghadap Internet, Anda dapat mengaitkan satu alamat IP Elastis per subnet secara opsional.

Saat Anda membuat grup target, Anda menentukan jenis targetnya, yang menentukan cara Anda mendaftarkan target. Misalnya, Anda dapat mendaftarkan ID instans, alamat IP, atau Application Load Balancer. Jenis target juga mempengaruhi apakah alamat IP klien dipertahankan. Untuk informasi selengkapnya, lihat the section called “Preservasi IP klien”.

Anda dapat menambah dan menghapus target dari penyeimbang beban saat kebutuhan Anda berubah, tanpa mengganggu keseluruhan aliran permintaan ke aplikasi Anda. 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.

Anda dapat mengonfigurasi pemeriksaan kondisi, yang digunakan untuk memantau kondisi target terdaftar sehingga penyeimbang beban hanya dapat mengirim permintaan ke target yang sehat.

Untuk informasi lebih lanjut, lihat Cara kerja Elastic Load Balancing di Panduan Pengguna Elastic Load Balancing.

Manfaat migrasi dari Classic Load Balancer

Menggunakan Penyeimbang Beban Jaringan dan bukan Classic Load Balancer memiliki keuntungan sebagai berikut:

- Kemampuan untuk menangani beban kerja yang mudah menguap dan skala untuk jutaan permintaan per detik.
- Support untuk alamat IP statis untuk penyeimbang beban. Anda juga dapat menetapkan satu alamat IP Elastis per subnet yang diaktifkan untuk penyeimbang beban.
- Support untuk mendaftarkan target berdasarkan alamat IP, termasuk target di luar VPC untuk penyeimbang beban.
- Support untuk permintaan peruteaan untuk beberapa aplikasi pada instans EC2 tunggal. Anda dapat mendaftarkan setiap instans atau alamat IP dengan kelompok target yang sama menggunakan beberapa port.
- Mendukung untuk aplikasi kontainer. Amazon Elastic Container Service (Amazon ECS) dapat memilih port yang tidak terpakai ketika penjadwalan tugas dan mendaftarkan tugas dengan grup target menggunakan port ini. Hal ini memungkinkan Anda untuk memanfaatkan klaster Anda secara efisien.
- Support untuk memantau kesehatan setiap layanan secara independen, karena pemeriksaan kesehatan ditentukan pada tingkat kelompok sasaran dan banyak CloudWatch metrik Amazon

dilaporkan pada tingkat kelompok sasaran. Melampirkan grup target ke grup Auto Scaling memungkinkan Anda untuk menskalakan setiap layanan dinamis berdasarkan permintaan.

Untuk informasi selengkapnya tentang fitur yang didukung oleh setiap jenis penyeimbang beban, lihat Perbandingan Produk untuk Elastic Load Balancing.

Bagaimana cara memulai

Untuk membuat Penyeimbang Beban Jaringan, cobalah salah satu tutorial berikut:

- Memulai dengan Penyeimbang Beban Jaringan
- Tutorial: Buat Penyeimbang Beban Jaringan menggunakan AWS CLI

Untuk demo konfigurasi penyeimbang beban umum, lihat Demo Elastic Load Balancing.

Harga

Untuk informasi selengkapnya, lihat Penyeimbang Beban Jaringan.

Memulai dengan Penyeimbang Beban Jaringan

Tutorial ini memberikan pengenalan langsung ke Network Load Balancers melalui AWS Management Console, antarmuka berbasis web. Untuk membuat Penyeimbang Beban Jaringan pertama Anda, selesaikan langkah berikut.

Tugas

Untuk demo konfigurasi penyeimbang beban umum, lihat Demo Elastic Load Balancing.

Sebelum Anda memulai

- Tentukan Availability Zone mana yang akan Anda gunakan untuk instans EC2 Anda. Konfigurasikan virtual private cloud (VPC) Anda dengan setidaknya satu subnet publik di masing-masing Availability Zone. Subnet publik ini digunakan untuk mengonfigurasi penyeimbang beban. Anda dapat meluncurkan instans EC2 Anda di subnet lain dari Availability Zone ini sebagai gantinya.
- Peluncuran setidaknya satu instans EC2 di setiap Availability Zone. Pastikan bahwa grup keamanan untuk instans ini memungkinkan akses TCP dari klien pada pendengar port dan pemeriksaan kesehatan permintaan dari VPC Anda. Untuk informasi selengkapnya, lihat Menargetkan grup keamanan.

Langkah 1: Konfigurasi grup target Anda

Buat grup target, yang digunakan dalam permintaan perutean. Aturan untuk rute pendengar Anda meminta ke target terdaftar dalam grup target ini. Penyeimbang beban memeriksa kesehatan target dalam up target ini menggunakan pengaturan pemeriksaan kesehatan yang ditetapkan untuk grup target.

Untuk mengonfigurasi grup 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 Buat grup target.
4. Pertahankan jenis target sebagai contoh.
5. Untuk nama grup Target, masukkan nama untuk grup target baru.
6. Untuk Protokol, pilih TCP, dan untuk Port, pilih 80.
7. Untuk VPC, pilih VPC yang berisi instance Anda.
8. Untuk Pemeriksaan kondisi, simpan pengaturan default.
9. Pilih Selanjutnya.
10. Pada halaman Daftarkan target, selesaikan langkah berikut. Ini adalah langkah opsional untuk membuat grup target. Namun, Anda harus mendaftarkan target Anda jika Anda ingin menguji penyeimbang beban Anda dan memastikan bahwa itu mengarahkan lalu lintas ke target Anda.
    a. Untuk Instans yang tersedia, pilih satu atau beberapa instans.
    b. Pertahankan port 80 default, dan pilih Sertakan sebagai tertunda di bawah ini.
11. Pilih Buat grup target.

Langkah 2: Pilih jenis penyeimbang beban

Elastic Load Balancing mendukung berbagai jenis penyeimbang beban. Untuk tutorial ini, Anda membuat Penyeimbang Beban Jaringan.

Untuk membuat Network Load Balancer menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada bilah navigasi, pilih Wilayah untuk penyeimbang beban Anda. Pastikan untuk memilih Wilayah yang sama dengan yang Anda gunakan untuk instans EC2 Anda.
3. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
4. Pilih Buat Penyeimbang Beban.
5. Untuk Penyeimbang Beban Jaringan, pilih Buat.

Langkah 3: Konfigurasi penyeimbang beban dan pendengar Anda

Untuk membuat Penyeimbang Beban Jaringan, Anda harus terlebih dahulu memberikan informasi konfigurasi dasar untuk penyeimbang beban Anda, seperti nama, skema, dan jenis alamat IP. Kemudian berikan informasi tentang jaringan Anda, dan satu atau lebih pendengar. Seorang pendengar adalah proses yang memeriksa permintaan koneksi. Listener dikonfigurasi dengan protokol dan port untuk koneksi dari klien ke penyeimbang beban. Untuk informasi selengkapnya tentang protokol dan port yang didukung, lihat Konfigurasi listener.

Untuk mengkonfigurasi penyeimbang beban dan pendengar Anda

1. Untuk Name penyeimbang beban, masukkan nama untuk penyeimbang beban Anda. Sebagai contoh, `my-nlb`.
2. Untuk Skema dan Jenis alamat IP, simpan nilai default.
3. Untuk pemetaan Jaringan, pilih VPC yang Anda gunakan untuk instans EC2 Anda. Untuk setiap Availability Zone yang Anda gunakan untuk meluncurkan instans EC2 Anda, pilih Availability Zone dan kemudian pilih satu subnet publik untuk Availability Zone tersebut.

   Secara default, AWS tetapkan alamat IPv4 ke setiap node penyeimbang beban dari subnet untuk Availability Zone-nya. Atau, saat Anda membuat penyeimbang beban menghadap internet, Anda dapat memilih alamat IP Elastis untuk setiap Availability Zone. Ini menyediakan penyeimbang beban Anda dengan alamat IP statis.
4. Untuk grup Keamanan, kami memilih grup keamanan default untuk VPC Anda. Anda dapat memilih grup keamanan lain sesuai kebutuhan. Jika Anda tidak memiliki grup keamanan yang sesuai, pilih Buat grup keamanan baru dan buat grup yang memenuhi kebutuhan keamanan Anda. Untuk informasi selengkapnya, lihat Membuat grup keamanan di Panduan Pengguna Amazon VPC.

   > **Warning**
   >
   > Jika Anda tidak mengaitkan grup keamanan apa pun dengan penyeimbang beban Anda sekarang, Anda tidak dapat mengaitkannya nanti.
5. Untuk Listener dan routing, pertahankan protokol dan port default, dan pilih grup target dari daftar. Ini mengonfigurasi pendengar yang menerima lalu lintas TCP pada port 80 dan meneruskan lalu lintas ke grup target yang dipilih secara default.

6. (Opsional) Tambahkan tag untuk mengkategorikan penyeimbang beban Anda. Tombol tag harus unik untuk setiap penyeimbang beban. Karakter yang diperbolehkan adalah huruf, spasi, dan angka (dalam UTF-8) dan karakter berikut: + - = . _ : / @. Jangan gunakan spasi awal dan akhir. Kunci dan nilai tag peka huruf besar dan kecil.
7. Tinjau konfigurasi Anda, dan pilih Buat penyeimbang beban. Beberapa atribut default diterapkan pada penyeimbang beban Anda selama pembuatan. Anda dapat melihat dan mengeditnya setelah membuat penyeimbang beban. Untuk informasi selengkapnya, lihat Atribut penyeimbang beban.

Langkah 4: Uji penyeimbang beban Anda

Setelah membuat penyeimbang beban, verifikasi bahwa itu mengirim lalu lintas ke instans EC2 Anda.

Untuk menguji penyeimbang beban Anda

1. Setelah Anda diberi tahu bahwa penyeimbang beban Anda berhasil dibuat, pilih Tutup.
2. Pada panel navigasi, di bawah Penyeimbang Beban, pilih Grup Target.
3. Pilih grup target yang baru dibuat.
4. Pilih Target dan verifikasi bahwa instans Anda sudah siap. Jika status instans Anda adalah `initial`, mungkin dikarenakan instans masih dalam proses mendaftar, atau belum lulus jumlah pemeriksaan kesehatan minimum untuk dianggap sehat. Setelah status setidaknya satu instans adalah `healthy`, Anda dapat menguji penyeimbang beban Anda.
5. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
6. Pilih nama penyeimbang beban yang baru dibuat untuk membuka halaman detailnya.
7. Salin nama DNS penyeimbang beban (misalnya, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). Tempelkan nama DNS ke bidang alamat browser web yang tersambung ke internet. Jika semuanya bekerja, peramban menampilkan halaman default server Anda.

Langkah 5: (Opsional) Hapus penyeimbang beban Anda

Segera setelah penyeimbang beban Anda tersedia, Anda akan dikenakan biaya untuk setiap jam atau sebagian jam yang Anda gunakan untuk menjalankan penyeimbang beban. Bila Anda tidak lagi memerlukan penyeimbang beban, Anda dapat menghapusnya. Segera setelah penyeimbang beban dihapus, Anda berhenti dikenakan biaya untuk itu. Perhatikan bahwa menghapus penyeimbang

beban tidak memengaruhi target yang terdaftar pada penyeimbang beban. Misalnya, instans EC2 Anda terus berjalan.

Untuk menghapus penyeimbang beban 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 kotak centang untuk penyeimbang beban, dan pilih Tindakan, Hapus.
4. Ketika diminta konfirmasi, masukkan **`confirm`** lalu pilih Hapus.

Tutorial: Buat Penyeimbang Beban Jaringan menggunakan AWS CLI

Tutorial ini memberikan pengenalan langsung untuk Penyeimbang Beban Jaringan melalui AWS CLI.

Sebelum Anda memulai

- Pasang AWS CLI atau perbarui ke versi aplikasi AWS CLI saat ini jika Anda menggunakan versi yang tidak mendukung Penyeimbang Beban Jaringan. Untuk informasi selengkapnya, lihat Menginstal AWS Command Line Interface dalam AWS Command Line Interface Panduan Penggunaan.
- Tentukan Availability Zone mana yang akan Anda gunakan untuk instans EC2 Anda. Konfigurasikan virtual private cloud (VPC) Anda dengan setidaknya satu subnet publik di masing-masing Availability Zone.
- Putuskan apakah Anda akan membuat penyeimbang beban IPv4 atau dualstack. Gunakan IPv4 jika Anda ingin klien berkomunikasi dengan penyeimbang beban hanya menggunakan alamat IPv4. Gunakan dualstack jika Anda ingin klien berkomunikasi dengan penyeimbang beban menggunakan alamat IPv4 dan IPv6. Anda juga dapat menggunakan dualstack untuk berkomunikasi dengan target backend, seperti aplikasi IPv6 atau subnet dualstack, menggunakan IPv6.
- Peluncuran setidaknya satu instans EC2 di setiap Availability Zone. Pastikan bahwa grup keamanan untuk instans ini memungkinkan akses TCP dari klien pada pendengar port dan pemeriksaan kesehatan permintaan dari VPC Anda. Untuk informasi selengkapnya, lihat Menargetkan grup keamanan.

Buat penyeimbang beban IPv4 Anda

Untuk membuat Load Balancer pertama Anda, selesaikan langkah berikut.

Untuk membuat penyeimbang beban IPv4

1. Gunakan create-load-balancerperintah untuk membuat penyeimbang beban IPv4, menentukan subnet publik untuk setiap Availability Zone tempat Anda meluncurkan instance. Anda hanya dapat menentukan satu subnet per Availability Zone.

Secara default, ketika Network Load Balancer dibuat menggunakanAWS CLI, mereka tidak secara otomatis menggunakan grup keamanan default untuk VPC. Jika Anda tidak mengaitkan grup keamanan apa pun dengan penyeimbang beban selama pembuatan, Anda tidak dapat menambahkannya nanti. Kami menyarankan Anda menentukan grup keamanan untuk penyeimbang beban Anda selama pembuatan dengan menggunakan `--security-groups` opsi.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
```

Ouput tersebut mencakup Amazon Resource Name (ARN) dari penyeimbang beban, dengan format berikut:

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

2. Gunakan create-target-groupperintah untuk membuat grup target IPv4, tentukan VPC yang sama dengan yang Anda gunakan untuk instans EC2 Anda. Kelompok target IPv4 mendukung target tipe IP dan instance.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-0598c7d356EXAMPLE
```

Luarannya mencakup ARN dari kelompok target, dengan format ini:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Gunakan perintah daftar-target 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 buat-pendengar untuk membuat pendengar untuk Load Balancer Anda dengan aturan default yang meneruskan permintaan ke grup target Anda:

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --
port 80  \
```

```
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Luaran berisi ARN pendengar, dengan format berikut:

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

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

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

Buat penyeimbang beban dualstack Anda

Untuk membuat Load Balancer pertama Anda, selesaikan langkah berikut.

Untuk membuat penyeimbang beban dualstack

1. Gunakan create-load-balancerperintah untuk membuat penyeimbang beban dualstack, menentukan subnet publik untuk setiap Availability Zone tempat Anda meluncurkan instance. Anda hanya dapat menentukan satu subnet per Availability Zone.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
```

   Keluaran tersebut mencakup penyeimbang beban Amazon Resource Name (ARN), dengan format berikut:

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

2. Gunakan create-target-groupperintah untuk membuat grup target, menentukan VPC yang sama yang Anda gunakan untuk instans EC2 Anda.

   Anda harus menggunakan grup target TCP atau TLS dengan penyeimbang beban dualstack Anda.

Anda dapat membuat grup target IPv4 dan IPv6 untuk diasosiasikan dengan penyeimbang beban dualstack. Jenis alamat IP grup target menentukan versi IP yang akan digunakan penyeimbang beban untuk berkomunikasi, dan memeriksa kesehatan, target backend Anda.

Kelompok target IPv4 mendukung target tipe IP dan instance. Target IPv6 hanya mendukung target IP.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-0598c7d356EXAMPLE  --ip-address-type [ipv4 or ipv6]
```

Luarannya mencakup ARN dari kelompok target, dengan format ini:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Gunakan perintah daftar-target 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 penyeimbang beban Anda dengan aturan default yang meneruskan permintaan ke grup target Anda. Dualstack load balancer harus memiliki pendengar TCP atau TLS.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --
port 80  \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Luaran berisi ARN pendengar, dengan format berikut:

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

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

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

Tentukan alamat IP Elastis untuk penyeimbang beban Anda

Saat Anda membuat Penyeimbang Beban Jaringa, Anda dapat menentukan satu alamat IP Elastis per subnet menggunakan pemetaan subnet.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \
--subnet-mappings SubnetId=subnet-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

Hapus penyeimbang beban Anda

Saat Anda tidak lagi memerlukan Load Balancer dan grup target, Anda dapat menghapusnya sebagai berikut:

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Penyeimbang Beban Jaringan

Sebuah Penyeimbang beban berfungsi sebagai titik kontak tunggal untuk klien. Klien mengirimkan permintaan ke penyeimbang beban, dan penyeimbang beban mengirimkannya ke target, seperti instans EC2, di satu atau beberapa Availability Zone.

Untuk mengkonfigurasi penyeimbang beban, Anda membuat Grup target, dan kemudian daftar target dengan kelompok target Anda. Penyeimbang beban Anda paling efektif jika Anda memastikan bahwa setiap Availability Zone yang diaktifkan memiliki setidaknya satu target yang terdaftar. Anda juga membuat pendengar untuk memeriksa permintaan koneksi dari klien dan merutekan permintaan dari klien ke target dalam grup target Anda.

Network Load Balancers mendukung koneksi dari klien melalui peering VPC, VPN AWS terkelola, dan solusi VPN pihak ketiga AWS Direct Connect.

Daftar Isi

Keadaan penyeimbang beban

Penyeimbang beban memiliki salah satu status berikut:

`provisioning`

Penyeimbang beban sedang disiapkan.

`active`

Penyeimbang beban telah sepenuhnya disiapkan dan siap untuk merutekan lalu lintas.

`failed`

Penyeimbang beban tidak dapat diatur.

Atribut penyeimbang beban

Load balancer memiliki atribut berikut:

`access_logs.s3.enabled`

Menunjukkan apakah log akses yang disimpan di Amazon S3 diaktifkan. Default-nya adalah `false`.

`access_logs.s3.bucket`

Nama bucket Amazon S3 untuk log akses. Atribut ini diperlukan jika log akses diaktifkan. Untuk informasi selengkapnya, lihat Persyaratan bucket.

`access_logs.s3.prefix`

Prefiks untuk lokasi di bucket Amazon S3.

`deletion_protection.enabled`

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

`ipv6.deny_all_igw_traffic`

Memblokir akses internet gateway (IGW) ke penyeimbang beban, mencegah akses yang tidak diinginkan ke penyeimbang beban internal Anda melalui gateway internet. Ini diatur `false` untuk penyeimbang beban yang menghadap ke internet dan `true` untuk penyeimbang beban internal. Atribut ini tidak mencegah akses internet non-IGW (misalnya, melalui peering, Transit Gateway AWS Direct Connect, atau). AWS VPN

`load_balancing.cross_zone.enabled`

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

`dns_record.client_routing_policy`

Menunjukkan bagaimana lalu lintas didistribusikan di antara Zona Ketersediaan penyeimbang beban. Nilai yang mungkin adalah `availability_zone_affinity` dengan afinitas zonal 100 persen, `partial_availability_zone_affinity` dengan 85 persen afinitas zonal, dan `any_availability_zone` dengan afinitas zona 0 persen.

Jenis alamat IP

Anda dapat mengatur jenis alamat IP yang dapat digunakan klien dengan penyeimbang beban Anda.

Network Load Balancers mendukung jenis alamat IP berikut:

`ipv4`

Klien harus terhubung ke penyeimbang beban menggunakan alamat IPv4 (misalnya, 192.0.2.1). Penyeimbang beban berkemampuan IPv4 (baik yang menghadap ke internet maupun internal) mendukung pendengar TCP, UDP, TCP_UDP, dan TLS.

`dualstack`

Klien dapat terhubung ke penyeimbang beban menggunakan alamat IPv4 (misalnya, 192.0.2.1) dan alamat IPv6 (misalnya, 2001:0db8:85a3:0:0:8a2e:0370:7334). Penyeimbang beban berkemampuan Dualstack (baik yang menghadap ke internet maupun internal) mendukung pendengar TCP dan TLS.

Pertimbangan

- Load balancer berkomunikasi dengan target berdasarkan jenis alamat IP dari kelompok target.
- Saat Anda mengaktifkan mode dualstack untuk penyeimbang beban, Elastic Load Balancing menyediakan catatan DNS AAAA untuk penyeimbang beban. Klien yang berkomunikasi dengan penyeimbang beban menggunakan alamat IPv4 menyelesaikan catatan DNS A. Klien yang berkomunikasi dengan penyeimbang beban menggunakan alamat IPv6 menyelesaikan catatan DNS AAAA.
- Akses ke penyeimbang beban dualstack internal Anda melalui gateway internet diblokir untuk mencegah akses internet yang tidak diinginkan. Namun, ini tidak mencegah akses internet lainnya (misalnya, melalui peering, Transit Gateway AWS Direct Connect, atau AWS VPN).

Untuk informasi selengkapnya tentang jenis alamat IP, lihatJenis alamat IP untuk Penyeimbang Beban Jaringan Anda.

Peta sumber daya Network Load Balancer

Peta sumber daya Network Load Balancer menyediakan tampilan interaktif arsitektur penyeimbang beban Anda, termasuk pendengar terkait, grup target, dan target. Peta sumber daya juga menyoroti hubungan dan jalur perutean antara semua sumber daya, menghasilkan representasi visual dari konfigurasi penyeimbang beban Anda.

Untuk melihat peta sumber daya Network Load Balancer menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih penyeimbang beban.
4. Pilih tab Resource map untuk menampilkan peta sumber daya penyeimbang beban.

Komponen peta sumber daya

Tampilan peta

Ada dua tampilan yang tersedia di peta sumber daya Network Load Balancer: Gambaran Umum, dan Peta Target Tidak Sehat. Ikhtisar dipilih secara default dan menampilkan semua sumber daya penyeimbang beban Anda. Memilih tampilan Peta Target Tidak Sehat hanya akan menampilkan target yang tidak sehat dan sumber daya yang terkait dengannya.

Tampilan Peta Target Tidak Sehat dapat digunakan untuk memecahkan masalah target yang gagal dalam pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat Memecahkan masalah target yang tidak sehat menggunakan peta sumber daya.

Kolom sumber daya

Peta sumber daya Network Load Balancer berisi tiga kolom sumber daya, satu untuk setiap jenis sumber daya. Grup sumber daya adalah Pendengar, grup Target, dan Target.

Ubin sumber daya

Setiap sumber daya dalam kolom memiliki ubin sendiri, yang menampilkan rincian tentang sumber daya tertentu.

- Melayang di atas ubin sumber daya menyoroti hubungan antara itu dan sumber daya lainnya.
- Memilih ubin sumber daya menyoroti hubungan antara itu dan sumber daya lainnya, dan menampilkan detail tambahan tentang sumber daya tersebut.
  - Ringkasan kesehatan kelompok sasaran: Jumlah target terdaftar untuk setiap status kesehatan.
  - status kesehatan target: Status dan deskripsi kesehatan target saat ini.

> **Note**
>
> Anda dapat menonaktifkan Tampilkan detail sumber daya untuk menyembunyikan detail tambahan dalam peta sumber daya.

- Setiap ubin sumber daya berisi tautan yang, ketika dipilih, menavigasi ke halaman detail sumber daya tersebut.
  - Pendengar - Pilih protokol pendengar: port. Misalnya, `TCP:80`
  - Grup sasaran - Pilih nama grup target. Misalnya, `my-target-group`
  - Target - Pilih ID target. Misalnya, `i-1234567890abcdef0`

Ekspor peta sumber daya

Memilih Ekspor memberi Anda opsi untuk mengekspor tampilan saat ini dari peta sumber daya Network Load Balancer Anda sebagai PDF.

Zona Ketersediaan

Anda mengaktifkan satu atau beberapa Availability Zone untuk penyeimbang beban saat membuatnya. Anda dapat mengaktifkan Penyeimbang Beban Jaringan dalam beberapa Availability Zone untuk meningkatkan toleransi kesalahan aplikasi Anda. Anda tidak dapat menonaktifkan Availability Zone untuk Network Load Balancer setelah membuatnya, tetapi Anda dapat mengaktifkan Availability Zone tambahan.

Saat Anda mengaktifkan Availability Zone untuk penyeimbang beban, Anda menentukan satu subnet dari Availability Zone tersebut. Elastic Load Balancing menciptakan simpul penyeimbang beban di Availability Zone dan antarmuka jaringan untuk subnet (deskripsi dimulai dengan "ELB net" dan mencakup nama penyeimbang beban). Setiap simpul penyeimbang beban di Availability Zone menggunakan antarmuka jaringan ini untuk mendapatkan alamat IPv4. Perhatikan bahwa Anda dapat melihat antarmuka jaringan ini tetapi Anda tidak dapat memodifikasinya.

Bila Anda membuat penyeimbang beban menghadap internet, Anda dapat menentukan satu alamat IP Elastis per subnet secara opsional. Jika Anda tidak memilih salah satu alamat IP Elastis Anda sendiri, Elastic Load Balancing menyediakan satu alamat IP Elastis per subnet untuk Anda. Alamat IP Elastis ini menyediakan penyeimbang beban Anda dengan alamat IP statis yang tidak akan berubah selama masa pakai penyeimbang beban. Anda tidak dapat mengubah alamat IP Elastis ini setelah Anda membuat penyeimbang beban.

Bila Anda membuat penyeimbang beban internal, Anda dapat menentukan satu alamat IP privat per subnet secara opsional. Jika Anda tidak menentukan alamat IP dari subnet, Elastic Load Balancing memilih satu untuk Anda. Alamat IP privat ini menyediakan penyeimbang beban Anda dengan alamat IP statis yang tidak akan berubah selama masa pakai penyeimbang beban. Anda tidak dapat mengubah alamat IP pribadi ini setelah Anda membuat penyeimbang beban.

Pertimbangan

- Untuk penyeimbang beban yang menghadap ke internet, subnet yang Anda tetapkan untuk penyeimbang beban harus memiliki setidaknya 8 alamat IP yang tersedia. Untuk penyeimbang beban internal, ini hanya diperlukan jika Anda mengizinkan AWS memilih alamat IPv4 pribadi dari subnet.
- Anda tidak dapat menentukan subnet di Availability Zone terbatas. Pesan kesalahannya adalah "Penyeimbang beban dengan jenis 'jaringan' tidak didukung di az_name". Anda dapat menentukan subnet di Availability Zone lain yang tidak dibatasi dan menggunakan lintas zona penyeimbang beban untuk mendistribusikan lalu lintas ke target di Availability Zone yang dibatasi.
- Anda dapat menentukan subnet yang dibagikan dengan Anda.
- Anda tidak dapat menentukan subnet di Zona Lokal.

Setelah Anda mengaktifkan Availability Zone, penyeimbang beban mulai merutekan permintaan ke target yang terdaftar di Availability Zone tersebut. Penyeimbang beban Anda paling efektif jika Anda memastikan bahwa setiap Availability Zone yang diaktifkan memiliki setidaknya satu target yang terdaftar.

Untuk menemukan Availability Zone Anda menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Pemetaan jaringan, pilih Edit subnet.

5. Untuk mengaktifkan Availability Zone, pilih kotak centang untuk Availability Zone tersebut. Jika ada satu subnet untuk Availability Zone itu, subnet tersebut dipilih. Jika ada lebih dari satu subnet untuk Availability Zone itu, pilih salah satu subnet. Perhatikan bahwa Anda dapat memilih paling banyak satu subnet per Availability Zone.

   Untuk penyeimbang beban yang menghadap ke internet, Anda dapat memilih alamat IP Elastis untuk setiap Availability Zone. Untuk penyeimbang beban internal, Anda dapat menetapkan alamat IP privat dari kisaran IPv4 dari setiap subnet dan bukan membiarkan Elastic Load Balancing menetapkan satu.
6. Pilih Simpan perubahan.

Untuk menambahkan Availability Zone menggunakan AWS CLI

Gunakan perintah set-subnet.

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 penyeimbang beban mendistribusikan lalu lintas di seluruh target terdaftar di semua Availability Zone yang diaktifkan. Anda juga dapat mengaktifkan penyeimbangan beban lintas zona di tingkat kelompok target. Untuk informasi selengkapnya, lihat the section called “Penyeimbangan beban lintas zona” dan Cross-zone load balancing di Panduan Pengguna Elastic Load Balancing.

Perlindungan penghapusan

Untuk mencegah penyeimbang beban terhapus secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghapusan. Secara default, perlindungan penghapusan dinonaktifkan untuk penyeimbang beban Anda.

Jika Anda mengaktifkan perlindungan penghapusan untuk penyeimbang beban, Anda harus menonaktifkannya sebelum dapat menghapus penyeimbang beban.

Untuk mengaktifkan perlindungan penghapusan menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.

4. Pada tab Atribut, pilih Edit.
5. Di bawah Konfigurasi, aktifkan Perlindungan penghapusan.
6. Pilih Simpan perubahan.

Untuk menonaktifkan perlindungan penghapusan menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Di bawah Konfigurasi, aktifkan Perlindungan penghapusan.
6. Pilih Simpan perubahan.

Untuk mengaktifkan atau menonaktifkan perlindungan penghapusan menggunakan AWS CLI

Gunakan perintah ubah-atribut-penyeimbang-beban dengan `deletion_protection.enabled` atribut.

Koneksi waktu habis

Untuk setiap permintaan TCP bahwa klien membuat melalui Penyeimbang Beban Jaringan, keadaan sambungan dilacak. Jika tidak ada data yang dikirim melalui sambungan oleh klien atau target untuk lebih lama dari waktu siaga habis, sambungan ditutup. Jika klien atau target mengirim data setelah periode timeout idle berlalu, ia menerima paket TCP RST untuk menunjukkan bahwa koneksi tidak lagi valid.

Kami menetapkan nilai batas waktu idle untuk aliran TCP menjadi 350 detik. Anda tidak dapat mengubah nilai ini. Klien atau target dapat menggunakan paket TCP keepalive untuk me-reset waktu siaga. Paket Keepalive yang dikirim untuk mempertahankan koneksi TLS tidak dapat berisi data atau payload.

Ketika pendengar TLS menerima paket TCP keepalive dari klien atau target, penyeimbang beban menghasilkan paket TCP keepalive dan mengirimkannya ke koneksi front-end dan back-end setiap 20 detik. Anda tidak dapat mengubah perilaku ini.

Sementara UDP tidak terhubung, penyeimbang beban mempertahankan status aliran UDP berdasarkan alamat dan port IP sumber dan tujuan. Ini memastikan bahwa paket yang termasuk

dalam aliran yang sama secara konsisten dikirim ke target yang sama. Setelah periode waktu habis siaga berlalu, penyeimbang beban menganggap paket UDP masuk sebagai aliran baru dan rute ke target baru. Elastic Load Balancing menetapkan nilai waktu tunggu idle untuk UDP mengalir ke 120 detik.

Instans EC2 harus menanggapi permintaan baru dalam waktu 30 detik untuk membangun jalan kembali.

Nama DNS

Setiap Penyeimbang Beban Jaringan menerima nama Sistem Nama Domain (DNS) default dengan sintaks berikut: *nama-id*.elb.*wilayah*.amazonaws.com. Misalnya, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com.

Jika Anda lebih suka menggunakan nama DNS yang lebih mudah diingat, Anda dapat membuat nama domain kustom dan mengaitkannya dengan nama DNS untuk penyeimbang beban Anda. Ketika klien membuat permintaan menggunakan nama domain kustom ini, DNS server menyelesaikan ke nama DNS untuk penyeimbang beban Anda.

Pertama, daftarkan nama domain dengan registrar nama domain terakreditasi. Selanjutnya, gunakan layanan DNS Anda, seperti registrar domain Anda, untuk membuat catatan DNS untuk merutekan permintaan ke penyeimbang beban Anda. Untuk informasi lebih lanjut, lihat dokumentasi untuk server DNS Anda. Misalnya, jika Anda menggunakan Amazon Route 53 sebagai layanan DNS, Anda membuat catatan alias yang menunjuk ke penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Merutekan lalu lintas ke penyeimbang beban ELB di Panduan Pengembang Amazon Route 53.

penyeimbang beban memiliki satu alamat IP per Availability Zone yang diaktifkan. Ini adalah alamat IP dari node penyeimbang beban. Nama DNS penyeimbang beban menyelesaikan ke alamat ini. Sebagai contoh, misalkan bahwa nama domain kustom untuk penyeimbang beban Anda adalah `example.networkloadbalancer.com`. Gunakan perintah berikut dig atau nslookup untuk menentukan alamat IP dari simpul penyeimbang beban.

Linux atau Mac

```
$ dig +short example.networkloadbalancer.com
```

Windows

```
C:\> nslookup example.networkloadbalancer.com
```

Penyeimbang beban memiliki catatan DNS untuk simpul penyeimbang beban. Anda dapat menggunakan nama DNS dengan sintaks berikut untuk menentukan alamat IP dari simpul penyeimbang beban: *az*.*nama*-*id*.elb.*wilayah*.amazonaws.com.

Linux atau Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Afinitas DNS Zona Ketersediaan

Saat menggunakan kebijakan perutean klien default, permintaan yang dikirim ke nama DNS Network Load Balancers Anda akan menerima alamat IP penyeimbang beban yang sehat. Ini mengarah pada distribusi koneksi klien di seluruh Zona Ketersediaan penyeimbang beban. Dengan kebijakan perutean afinitas Availability Zone, kueri DNS klien mendukung alamat IP penyeimbang beban di Availability Zone mereka sendiri. Ini membantu meningkatkan latensi dan ketahanan, karena klien tidak perlu melewati batas Availability Zone saat menghubungkan ke target.

Kebijakan perutean klien tersedia untuk Network Load Balancers menggunakan resolver Route 53:

- Afinitas Zona Ketersediaan - afinitas zona 100 persen

  Kueri DNS klien akan mendukung alamat IP penyeimbang beban di Availability Zone mereka sendiri. Pertanyaan dapat diselesaikan ke zona lain jika tidak ada alamat IP penyeimbang beban yang sehat di zona mereka sendiri.
- Afinitas Zona Ketersediaan Sebagian — 85 persen afinitas zona

  85 persen kueri DNS klien akan mendukung alamat IP penyeimbang beban di Availability Zone mereka sendiri, sementara kueri yang tersisa diselesaikan ke zona sehat mana pun. Pertanyaan dapat diselesaikan ke zona sehat lainnya jika tidak ada IP sehat di zona mereka. Ketika tidak ada IP yang sehat di zona mana pun, kueri diselesaikan ke zona mana pun.
- Setiap Availability Zone (default) - 0 persen afinitas zona

  Kueri DNS klien diselesaikan di antara alamat IP penyeimbang beban yang sehat di semua Zona Ketersediaan penyeimbang beban.

> **Note**
>
> Kebijakan perutean afinitas Availability Zone hanya berlaku untuk klien yang menyelesaikan nama DNS Network Load Balancers menggunakan Resolver Route 53. Untuk informasi selengkapnya, lihat Apa itu Amazon Route 53 Resolver? di Panduan Pengembang Amazon Route 53

Afinitas Availability Zone membantu merutekan permintaan dari klien ke penyeimbang beban, sedangkan penyeimbangan beban lintas zona digunakan untuk membantu merutekan permintaan dari penyeimbang beban ke target. Saat menggunakan afinitas Availability Zone, penyeimbangan beban lintas zona harus dimatikan, ini memastikan lalu lintas penyeimbang beban dari klien ke target tetap berada dalam Availability Zone yang sama. Dengan konfigurasi ini, lalu lintas klien dikirim ke Zona Ketersediaan Network Load Balancer yang sama, jadi disarankan untuk mengonfigurasi aplikasi Anda agar diskalakan secara independen di setiap Availability Zone. Ini merupakan pertimbangan penting ketika jumlah klien per zona ketersediaan, atau lalu lintas per Availability Zone tidak sama. Untuk informasi selengkapnya, lihat Penyeimbangan beban lintas zona untuk kelompok sasaran.

Ketika Availability Zone dianggap tidak sehat, atau ketika pergeseran zona dimulai, alamat IP zonal akan dianggap tidak sehat dan tidak dikembalikan ke klien kecuali gagal terbuka berlaku. Afinitas Availability Zone dipertahankan ketika catatan DNS gagal dibuka. Ini membantu menjaga Availability Zone tetap independen dan mencegah potensi kegagalan lintas zona.

Saat menggunakan afinitas Availability Zone, waktu ketidakseimbangan antara Availability Zone diharapkan. Disarankan untuk memastikan target Anda menskalakan pada tingkat zona, untuk mendukung setiap beban kerja Availability Zones. Dalam kasus di mana ketidakseimbangan ini signifikan, disarankan untuk mematikan afinitas Availability Zone. Hal ini memungkinkan pemerataan koneksi klien antara semua penyeimbang beban Availability Zones dalam waktu 60 detik, atau DNS TTL.

Sebelum menggunakan afinitas Availability Zone, pertimbangkan hal berikut:

- Afinitas Availability Zone menyebabkan perubahan pada semua klien Network Load Balancers yang menggunakan Resolver Route 53.
  - Klien tidak dapat memutuskan antara resolusi DNS zonal-lokal dan multi-zona. Afinitas Zona Ketersediaan memutuskan untuk mereka.

  - Klien tidak diberikan metode yang andal untuk menentukan kapan mereka dipengaruhi oleh afinitas Availability Zone, atau cara mengetahui alamat IP mana yang ada di Availability Zone.
- Klien akan tetap ditugaskan ke alamat IP zona-lokal mereka sampai dianggap sepenuhnya tidak sehat menurut pemeriksaan kesehatan DNS, dan dihapus dari DNS.
- Menggunakan afinitas Availability Zone dengan penyeimbangan beban lintas zona aktif dapat menyebabkan distribusi koneksi klien yang tidak seimbang antara Availability Zones. Disarankan untuk mengonfigurasi tumpukan aplikasi Anda untuk menskalakan secara independen di setiap Availability Zone, memastikannya dapat mendukung lalu lintas klien zona.
- Jika penyeimbangan beban lintas zona aktif, Network Load Balancer dapat terkena dampak lintas zona.
- Beban pada masing-masing Zona Ketersediaan Penyeimbang Beban Jaringan akan sebanding dengan lokasi zona permintaan klien. Jika Anda tidak mengonfigurasi berapa banyak klien yang berjalan di Availability Zone mana, Anda harus secara independen menskalakan setiap Availability Zone secara reaktif.

Pemantauan

Disarankan untuk melacak distribusi koneksi antara Availability Zones, menggunakan metrik penyeimbang beban zonal. Anda dapat menggunakan metrik untuk melihat jumlah koneksi baru dan aktif per zona.

Kami merekomendasikan untuk melacak hal-hal berikut:

- **`ActiveFlowCount`**— Jumlah total arus bersamaan (atau koneksi) dari klien ke target.
- **`NewFlowCount`**— Jumlah total arus baru (atau koneksi) yang ditetapkan dari klien ke target dalam periode waktu tersebut.
- **`HealthyHostCount`**Jumlah target yang dianggap sehat.
- **`UnHealthyHostCount`**Jumlah target yang dianggap tidak sehat.

Untuk informasi selengkapnya, lihat CloudWatch metrik untuk Network Load Balancer

Aktifkan afinitas Availability Zone

Langkah-langkah dalam prosedur ini menjelaskan cara mengaktifkan afinitas Availability Zone menggunakan konsol Amazon EC2.

Untuk mengaktifkan afinitas Availability Zone menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Di bawah konfigurasi perutean Zona Ketersediaan, Kebijakan perutean klien (catatan DNS), pilih afinitas Zona Ketersediaan atau afinitas Zona Ketersediaan Sebagian.
6. Pilih Simpan perubahan.

Untuk mengaktifkan afinitas Availability Zone menggunakan AWS CLI

Gunakan perintah modify-load-balancer-attributes dengan atribut `dns_record.client_routing_policy`.

Matikan afinitas Availability Zone

Langkah-langkah dalam prosedur ini menjelaskan cara mematikan afinitas Availability Zone menggunakan konsol Amazon EC2.

Untuk mematikan afinitas Availability Zone menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Di bawah konfigurasi perutean Availability Zone, Kebijakan perutean klien (catatan DNS), pilih Ay Availability Zone.
6. Pilih Simpan perubahan.

Untuk menonaktifkan afinitas Availability Zone menggunakan AWS CLI

Gunakan perintah modify-load-balancer-attributes dengan atribut `dns_record.client_routing_policy`.

Buat Penyeimbang Beban Jaringan

Penyeimbang beban menerima permintaan dari klien dan mendistribusikannya ke seluruh target dalam grup target, seperti instans EC2.

Sebelum memulai, pastikan bahwa virtual private cloud (VPC) untuk penyeimbang beban Anda memiliki setidaknya satu subnet publik di setiap Availability Zone di mana Anda memiliki target. Anda juga harus mengkonfigurasi grup target dan mendaftarkan setidaknya satu target untuk ditetapkan sebagai default untuk merutekan lalu lintas Anda ke grup target.

Untuk membuat penyeimbang beban menggunakan AWS CLI, lihatTutorial: Buat Penyeimbang Beban Jaringan menggunakan AWS CLI.

Untuk membuat penyeimbang beban menggunakan AWS Management Console, selesaikan tugas-tugas berikut.

Tugas

- Langkah 1: Mengkonfigurasi grup target
- Langkah 2: Daftarkan target
- Langkah 3: Mengkonfigurasi penyeimbang beban dan pendengar
- Langkah 4: Uji penyeimbang beban

Langkah 1: Mengkonfigurasi grup target

Mengkonfigurasi grup target memungkinkan Anda untuk mendaftarkan target seperti instans EC2. Grup target yang Anda mengkonfigurasi dalam langkah ini digunakan sebagai grup target dalam aturan pendengar saat Anda mengkonfigurasi penyeimbang beban. Untuk informasi selengkapnya, lihat Target grup untuk Penyeimbang Beban Jaringan Anda.

Untuk mengonfigurasi grup target Anda menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Target Groups.
3. PilihBuat grup target.
4. Untuk panel konfigurasi Dasar, lakukan hal berikut:

a. Untuk Pilih jenis target, pilih Instans untuk mendaftarkan target berdasarkan ID instans, alamat IP untuk mendaftarkan target berdasarkan alamat IP, atau Application Load Balancer untuk mendaftarkan Application Load Balancer sebagai target.

b. Untuk Name, masukkan nama untuk grup target.

c. Untuk Protokol, pilih protokol seperti berikut:

   - Jika protokol pendengar adalah TCP, pilih TCP atau TCP_UDP.
   - Jika protokol pendengar adalah TLS, pilih TCP atau TLS.
   - Jika protokol pendengar adalah UDP, pilih UDP atau TCP_UDP.
   - Jika protokol pendengar adalah TCP_UDP, pilih TCP_UDP.

d. (Opsional) Untuk Port, mengubah nilai default yang diperlukan.

e. Untuk jenis alamat IP, pilih IPv4 atau IPv6. Opsi ini hanya tersedia jika jenis targetnya adalah Instans atau alamat IP dan protokolnya adalah TCP atau TLS.

   Anda harus mengaitkan grup target IPv6 dengan penyeimbang beban dualstack. Semua target dalam kelompok target harus memiliki jenis alamat IP yang sama. Anda tidak dapat mengubah jenis alamat IP grup target setelah Anda membuatnya.

f. Untuk VPC, pilih virtual private cloud (VPC) dengan target yang akan didaftarkan.

5. Untuk panel Pemeriksaan Kesehatan, ubah pengaturan default sesuai kebutuhan. Untuk pengaturan pemeriksaan kesehatan lanjutan, pilih port pemeriksaan kesehatan, hitungan, batas waktu, interval, dan kode keberhasilan. 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) Untuk menambahkan tag, perluas Tag, pilih Tambahkan tag, dan masukkan kunci tag dan nilai tag.

7. Pilih Selanjutnya.

Langkah 2: Daftarkan target

Anda dapat mendaftarkan instans EC2, alamat IP, atau Application Load Balancer dengan grup target Anda. Ini adalah langkah opsional untuk membuat penyeimbang beban. Namun, Anda harus

mendaftarkan target Anda untuk memastikan bahwa penyeimbang beban Anda dapat mengarahkan lalu lintas ke mereka.

1. Pada halaman Daftar target, tambahkan satu atau beberapa target sebagai berikut:
   - Jika jenis targetnya adalah Instans, pilih instance, masukkan port, lalu pilih Sertakan sebagai tertunda di bawah ini.
   - Jika jenis target adalah alamat IP, pilih jaringan, masukkan alamat IP dan port, lalu pilih Sertakan sebagai tertunda di bawah ini.
   - Jika jenis targetnya adalah Application Load Balancer, pilih Application Load Balancer.
2. Pilih Buat grup target.

Langkah 3: Mengkonfigurasi penyeimbang beban dan pendengar

Untuk membuat Penyeimbang Beban Jaringan, Anda harus terlebih dahulu memberikan informasi konfigurasi dasar untuk penyeimbang beban Anda, seperti nama, skema, dan jenis alamat IP. Kemudian berikan informasi tentang jaringan Anda dan satu atau lebih pendengar. Listener adalah proses yang memeriksa permintaan koneksi. Listener dikonfigurasi dengan protokol dan port untuk koneksi dari klien ke penyeimbang beban. Untuk informasi selengkapnya tentang protokol dan port yang didukung, lihat Konfigurasi listener.

Untuk mengonfigurasi penyeimbang beban dan pendengar menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih Buat Penyeimbang Beban.
4. Di bawah Penyeimbang Beban Jaringan, pilih Buat.
5. Konfigurasi dasar
   a. Untuk Name, masukkan nama untuk penyeimbang beban Anda. Sebagai contoh, **`my-nlb`**. Nama Network Load Balancer Anda harus unik dalam rangkaian Application Load Balancers dan Network Load Balancer untuk Wilayah tersebut. Ini dapat memiliki maksimal 32 karakter, dan hanya berisi karakter alfanumerik dan tanda hubung. Itu tidak boleh dimulai atau diakhiri dengan tanda hubung, atau dengan. `internal-`
   b. Untuk Skema, pilih Mengakses Internet atau Internal. Penyeimbang beban yang menghadap ke internet merutekan permintaan dari klien ke target melalui internet. Pengimbang beban internal merutekan permintaan ke target menggunakan alamat IP privat.

c. Untuk jenis alamat IP, pilih IPv4 jika klien Anda menggunakan alamat IPv4 untuk berkomunikasi dengan penyeimbang beban atau Dualstack jika klien Anda menggunakan alamat IPv4 dan IPv6 untuk berkomunikasi dengan penyeimbang beban.

6. Pemetaan jaringan

   a. Untuk VPC, pilih VPC yang Anda gunakan untuk instans EC2 Anda.

      Jika Anda memilih Mengakses Internet untuk Skema, hanya VPC dengan internet gateway yang tersedia untuk dipilih.

   b. Untuk Pemetaan, Pilih satu atau beberapa Availability Zone dan subnet yang sesuai. Mengaktifkan beberapa Availability Zone meningkatkan toleransi kesalahan aplikasi Anda. Anda dapat menentukan subnet yang dibagikan dengan Anda.

      Untuk penyeimbang beban mengakses internet, Anda dapat memilih alamat IP Elastis untuk setiap Availability Zone. Ini menyediakan penyeimbang beban Anda dengan alamat IP statis. Atau, untuk penyeimbang beban internal, Anda dapat menetapkan alamat IP pribadi dari rentang IPv4 setiap subnet alih-alih membiarkan AWS menetapkan satu untuk Anda.

7. Untuk grup Keamanan, kami memilih grup keamanan default untuk VPC Anda. Anda dapat memilih grup keamanan lain sesuai kebutuhan. Jika Anda tidak memiliki grup keamanan yang sesuai, pilih Buat grup keamanan baru dan buat grup yang memenuhi kebutuhan keamanan Anda. Untuk informasi selengkapnya, lihat Membuat grup keamanan di Panduan Pengguna Amazon VPC.

   > **Warning**
   >
   > Jika Anda tidak mengaitkan grup keamanan apa pun dengan penyeimbang beban Anda sekarang, Anda tidak dapat mengaitkannya nanti.

8. Pendengar dan perutean

   a. Defaultnya adalah pendengar yang menerima lalu lintas TCP pada port 80. Anda dapat menyimpan pengaturan pendengar default, atau memodifikasi Protokol dan Port sesuai kebutuhan.

   b. Untuk Tindakan Bawaan, pilih grup target untuk meneruskan lalu lintas. Jika Anda tidak membuat grup target sebelumnya, Anda harus membuatnya sekarang. Anda dapat memilih Tambahkan pendengar untuk menambahkan pendengar lain (misalnya, pendengar TLS).

   c. (Opsional) Tambahkan tag untuk mengkategorikan pendengar Anda.

d. Untuk pengaturan pendengar Aman (hanya tersedia untuk pendengar TLS), lakukan hal berikut:

   i. Untuk kebijakan Keamanan, pilih kebijakan keamanan yang memenuhi persyaratan Anda.

   ii. Untuk Kebijakan ALPN, pilih kebijakan untuk mengaktifkan ALPN atau pilih Tidak ada untuk menonaktifkan ALPN.

   iii. Untuk Sertifikat SSL Default, pilih Dari ACM (disarankan) dan pilih sertifikat. Jika Anda tidak memiliki sertifikat yang tersedia, Anda dapat mengimpor sertifikat ke ACM atau menggunakan ACM untuk menyediakannya untuk Anda. Untuk informasi selengkapnya, lihat Menerbitkan dan mengelola sertifikat di Panduan AWS Certificate Manager Pengguna.

9. (Opsional) Anda dapat menggunakan layanan Add-on dengan penyeimbang beban Anda. Misalnya, Anda dapat memilih untuk AWS Global Acceleratormembuat akselerator untuk Anda dan mengaitkan penyeimbang beban Anda dengan akselerator. Nama akselerator dapat memiliki karakter berikut (hingga 64 karakter): a-z, A-Z, 0-9,. (periode), dan - (tanda hubung). Setelah akselerator dibuat, buka AWS Global Acceleratorkonsol untuk menyelesaikan konfigurasinya. Untuk informasi selengkapnya, lihat Menambahkan akselerator saat Anda membuat penyeimbang beban

10. Tanda

    (Opsional) Tambahkan tag untuk mengkategorikan penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Tag.

11. Ringkasan

    Tinjau konfigurasi Anda, dan pilih Buat penyeimbang beban. Beberapa atribut default diterapkan pada penyeimbang beban Anda selama pembuatan. Anda dapat melihat dan mengeditnya setelah membuat penyeimbang beban. Untuk informasi selengkapnya, lihat Atribut penyeimbang beban.

Langkah 4: Uji penyeimbang beban

Setelah membuat penyeimbang beban, Anda dapat memverifikasi bahwa instans EC2 Anda telah lulus pemeriksaan kesehatan awal, dan kemudian menguji apakah penyeimbang beban mengirimkan lalu lintas ke instans EC2 Anda. Untuk menghapus penyeimbang beban, lihat Menghapus Penyeimbang Beban Jaringan.

Untuk menguji penyeimbang beban

1. Setelah penyeimbang beban dibuat, pilih Tutup.
2. Di panel navigasi kiri, pilih Grup Target.
3. Pilih grup target baru.
4. Pilih Target dan verifikasi bahwa instans Anda sudah siap. Jika status instans adalah`initial`, itu mungkin karena instance masih dalam proses terdaftar atau belum lulus jumlah minimum pemeriksaan kesehatan untuk dianggap sehat. Setelah status setidaknya satu instans sehat, Anda dapat menguji penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Status kondisi target.
5. Di panel navigasi, pilih Load Balancers.
6. Pilih penyeimbang beban baru.
7. Salin nama DNS penyeimbang beban (misalnya, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). Tempelkan nama DNS ke bidang alamat browser web yang tersambung ke internet. Jika semuanya berfungsi, browser menampilkan halaman default server Anda.

Jenis alamat IP untuk Penyeimbang Beban Jaringan Anda

Anda dapat mengonfigurasi Network Load Balancer Anda sehingga klien dapat berkomunikasi dengan penyeimbang beban 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.

Persyaratan dualstack

- Anda dapat mengatur jenis alamat IP saat membuat penyeimbang beban dan memperbaruinya kapan saja.
- Virtual private cloud (VPC) dan subnet yang Anda tentukan untuk penyeimbang beban harus memiliki blok CIDR IPv6 terkait. Untuk informasi selengkapnya, lihat alamat IPv6 alamat dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.
- Penyeimbang beban hanya harus memiliki pendengar TCP dan TLS.
- Tabel rute untuk subnet penyeimbang beban harus rute lalu lintas IPv6.
- ACL jaringan untuk subnet penyeimbang beban mesti mengizinkan lalu lintas IPv6.

Untuk menetapkan jenis alamat IP pada penciptaan

Mengkonfigurasi pengaturan seperti yang dijelaskan di Membuat penyeimbang beban.

Untuk memperbarui jenis alamat IP menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih kotak centang untuk penyeimbang beban.
4. Pilih Actions, Edit IP address type.
5. Untuk jenis alamat IP, pilih IPv4 untuk mendukung alamat IPv4 saja atau Dualstack untuk mendukung alamat IPv4 dan IPv6.
6. Pilih Simpan perubahan.

Untuk memperbarui jenis alamat IP menggunakan AWS CLI

Gunakan perintah set-ip-address-type.

Grup keamanan untuk Network Load Balancer

Anda dapat mengaitkan grup keamanan dengan Network Load Balancer Anda untuk mengontrol lalu lintas yang diizinkan untuk mencapai dan meninggalkan penyeimbang beban. Anda menentukan port, protokol, dan sumber untuk memungkinkan lalu lintas masuk dan port, protokol, dan tujuan untuk memungkinkan lalu lintas keluar. Jika Anda tidak menetapkan grup keamanan ke penyeimbang beban Anda, semua lalu lintas klien dapat mencapai pendengar penyeimbang beban dan semua lalu lintas dapat meninggalkan penyeimbang beban.

Anda dapat menambahkan aturan ke grup keamanan yang terkait dengan target Anda yang mereferensikan grup keamanan yang terkait dengan Network Load Balancer Anda. Ini memungkinkan klien untuk mengirim lalu lintas ke target Anda melalui penyeimbang beban Anda, tetapi mencegah mereka mengirim lalu lintas langsung ke target Anda. Mereferensikan grup keamanan yang terkait dengan Network Load Balancer Anda di grup keamanan yang terkait dengan target Anda memastikan bahwa target Anda menerima lalu lintas dari penyeimbang beban meskipun Anda mengaktifkan pelestarian IP klien untuk penyeimbang beban Anda.

Anda tidak dikenakan biaya untuk lalu lintas yang diblokir oleh aturan grup keamanan masuk.

Daftar Isi

Pertimbangan

- Anda dapat mengaitkan grup keamanan dengan Network Load Balancer saat membuatnya. Jika Anda membuat Network Load Balancer tanpa mengaitkan grup keamanan apa pun, Anda tidak dapat mengaitkannya dengan penyeimbang beban nanti. Kami menyarankan Anda mengaitkan grup keamanan dengan penyeimbang beban saat Anda membuatnya.
- Setelah membuat Network Load Balancer dengan grup keamanan terkait, Anda dapat mengubah grup keamanan yang terkait dengan penyeimbang beban kapan saja.
- Pemeriksaan kesehatan tunduk pada aturan keluar, tetapi tidak aturan masuk. Anda harus memastikan bahwa aturan keluar tidak memblokir lalu lintas pemeriksaan kesehatan. Jika tidak, penyeimbang beban menganggap target tidak sehat.
- Anda dapat mengontrol apakah PrivateLink lalu lintas tunduk pada aturan masuk. Jika Anda mengaktifkan aturan masuk pada PrivateLink lalu lintas, sumber lalu lintas adalah alamat IP pribadi klien, bukan antarmuka titik akhir.

Contoh: Filter lalu lintas klien

Aturan masuk berikut dalam grup keamanan yang terkait dengan Network Load Balancer Anda hanya mengizinkan lalu lintas yang berasal dari rentang alamat yang ditentukan. Jika ini adalah penyeimbang beban internal, Anda dapat menentukan rentang CIDR VPC sebagai sumber untuk mengizinkan hanya lalu lintas dari VPC tertentu. Jika ini adalah penyeimbang beban yang menghadap ke internet yang harus menerima lalu lintas dari mana saja di internet, Anda dapat menentukan 0.0.0.0/0 sebagai sumbernya.

Ke dalam

Protokol	Sumber	Rentang port	Komentar
protokol	*rentang alamat IP klien*	*port pendengar*	Mengizinkan lalu lintas masuk dari CIDR sumber di port pendengar
ICMP	0.0.0.0/0	Semua	Memungkinkan lalu lintas ICMP masuk untuk mendukung MTU atau Path MTU Discovery †

† Untuk informasi selengkapnya, lihat Path MTU Discovery di Panduan Pengguna Amazon EC2.

Ke luar

Protokol	Tujuan	Rentang port	Komentar
Semua	Dimanapun	Semua	Mengizinkan semua lalu lintas ke luar

Contoh: Terima lalu lintas hanya dari penyeimbang beban

Misalkan Network Load Balancer Anda memiliki grup keamanan sg-111112222233333. Gunakan aturan berikut dalam grup keamanan yang terkait dengan instans target Anda untuk memastikan bahwa mereka hanya menerima lalu lintas dari Network Load Balancer. Anda harus memastikan bahwa target menerima lalu lintas dari penyeimbang beban di port target dan port pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat the section called “Menargetkan grup keamanan”.

Ke dalam

Protokol	Sumber	Rentang port	Komentar
protokol	sg-111112222233333	*port target*	Memungkinkan lalu lintas masuk dari penyeimbang beban pada port target
protokol	sg-111112222233333	*pemeriksaan kesehatan*	Memungkinkan lalu lintas masuk dari penyeimbang beban di port pemeriksaan kesehatan

Ke luar

Protokol	Tujuan	Rentang port	Komentar
Semua	Dimanapun	Setiap	Mengizinkan semua lalu lintas ke luar

Memperbarui grup keamanan terkait

Jika Anda mengaitkan setidaknya satu grup keamanan dengan penyeimbang beban saat Anda membuatnya, Anda dapat memperbarui grup keamanan untuk penyeimbang beban tersebut kapan saja.

Untuk memperbarui grup keamanan 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. Pada tab Keamanan, pilih Edit.
5. Untuk mengaitkan grup keamanan dengan penyeimbang beban Anda, pilih grup tersebut. Untuk menghapus grup keamanan dari penyeimbang beban, hapus grup tersebut.
6. Pilih Simpan perubahan.

Untuk memperbarui grup keamanan menggunakan AWS CLI

Gunakan perintah set-security-groups.

Perbarui pengaturan keamanan

Secara default, kami menerapkan aturan grup keamanan masuk ke semua lalu lintas yang dikirim ke penyeimbang beban. Namun, Anda mungkin tidak ingin menerapkan aturan ini ke lalu lintas yang dikirim ke penyeimbang beban AWS PrivateLink, yang dapat berasal dari alamat IP yang tumpang tindih. Dalam hal ini, Anda dapat mengonfigurasi penyeimbang beban sehingga kami tidak menerapkan aturan masuk untuk lalu lintas yang dikirim ke penyeimbang beban melalui. AWS PrivateLink

Untuk memperbarui pengaturan keamanan 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. Pada tab Keamanan, pilih Edit.
5. Di bawah pengaturan Keamanan, hapus Menegakkan aturan masuk tentang PrivateLink lalu lintas.
6. Pilih Simpan perubahan.

Untuk memperbarui pengaturan keamanan menggunakan AWS CLI

Gunakan perintah set-security-groups.

Pantau kelompok keamanan penyeimbang beban

Gunakan `SecurityGroupBlockedFlowCount_Outbound` CloudWatch metrik `SecurityGroupBlockedFlowCount_Inbound` dan untuk memantau jumlah aliran yang diblokir oleh grup keamanan penyeimbang beban. Lalu lintas yang diblokir tidak tercermin dalam metrik lain. Untuk informasi selengkapnya, lihat the section called “CloudWatch metrik”.

Gunakan log aliran VPC untuk memantau lalu lintas yang diterima atau ditolak oleh grup keamanan penyeimbang beban. Untuk informasi selengkapnya, lihat Log aliran VPC di Panduan Pengguna Amazon VPC.

Metrik untuk Penyeimbang Beban Jaringan Anda

Tag membantu Anda mengkategorikan penyeimbang beban Anda dengan berbagai cara. Misalnya, Anda dapat menandai sumber daya berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap penyeimbang beban. 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 penyeimbang beban 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 prefiks ini tidak dihitung terhadap tag Anda per batas sumber daya.

Untuk memperbarui tag untuk penyeimbang beban menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Di bagian tab Tanda, pilih Kelola tanda.
5. Untuk menambahkan tag, pilih Tambahkan tag dan masukkan kunci tag dan nilai tag. Karakter yang diperbolehkan adalah huruf, spasi, dan angka (dalam UTF-8) dan karakter berikut: + - = . _ : / @. Jangan gunakan spasi awal dan akhir. Kunci dan nilai tag peka huruf besar dan kecil.
6. Untuk memperbarui tag, masukkan nilai baru di Kunci dan Nilai.
7. Untuk menghapus tag, pilih tombol Hapus di sebelah tag.
8. Setelah selesai, pilih Simpan perubahan.

Untuk memperbarui tag untuk penyeimbang beban menggunakan AWS CLI

Gunakan perintah tambah-tag dan hapus-tag.

Menghapus Penyeimbang Beban Jaringan

Segera setelah penyeimbang beban Anda tersedia, Anda akan ditagih untuk setiap jam atau sebagian jam agar tetap berjalan. Saat tidak lagi membutuhkan penyeimbang beban, Anda dapat menghapusnya. Segera setelah penyeimbang beban dihapus, Anda berhenti dikenakan biaya untuk penyeimbang beban tersebut.

Anda tidak dapat menghapus penyeimbang beban jika perlindungan penghapusan diaktifkan. Untuk informasi selengkapnya, lihat Perlindungan penghapusan.

Anda tidak dapat menghapus penyeimbang beban jika digunakan oleh layanan lain. Sebagai contoh, jika penyeimbang beban dikaitkan dengan layanan VPC endpoint, Anda harus menghapus konfigurasi layanan endpoint sebelum Anda dapat menghapus penyeimbang beban terkait.

Menghapus penyeimbang beban juga menghapus pendengarnya. Menghapus penyeimbang beban tidak mempengaruhi target yang terdaftar. Misalnya, intans EC2 Anda terus berjalan dan masih terdaftar ke kelompok target mereka. Untuk menghapus grup target Anda, lihat Menghapus grup target.

Untuk menghapus penyeimbang beban menggunakan konsol

1. Jika Anda memiliki catatan DNS untuk domain Anda yang mengarah ke penyeimbang beban Anda, arahkan ke lokasi baru dan tunggu perubahan DNS diterapkan sebelum menghapus penyeimbang beban Anda.

   Contoh:

   - Jika rekaman adalah rekaman CNAME dengan Time To Live (TTL) 300 detik, tunggu setidaknya 300 detik sebelum melanjutkan ke langkah berikutnya.
   - Jika catatan adalah catatan Route 53 Alias (A), tunggu setidaknya 60 detik.
   - Jika menggunakan Route 53, perubahan catatan membutuhkan waktu 60 detik untuk menyebar ke semua server nama Route 53 global. Tambahkan waktu ini ke nilai TTL dari catatan yang sedang diperbarui.
2. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
3. Di panel navigasi, pilih Load Balancers.
4. Pilih kotak centang untuk penyeimbang beban.
5. Pilih Tindakan, Hapus penyeimbang beban.
6. Ketika diminta konfirmasi, masukkan **`confirm`** lalu pilih Hapus.

Untuk menghapus penyeimbang beban menggunakan AWS CLI

Gunakan perintah delete-load-balancer.

Pergeseran zona

Zonal shift adalah kemampuan di Amazon Route 53 Application Recovery Controller (Route 53 ARC). Dengan pergeseran zona, Anda dapat mengalihkan sumber daya penyeimbang beban

dari Availability Zone yang terganggu dengan satu tindakan. Dengan cara ini, Anda dapat terus beroperasi dari Availability Zone sehat lainnya di file Wilayah AWS.

Saat Anda memulai pergeseran zona, penyeimbang beban Anda berhenti mengirimkan lalu lintas untuk sumber daya ke Availability Zone yang terpengaruh. Route 53 ARC segera menciptakan pergeseran zona. Namun, dibutuhkan waktu singkat, biasanya hingga beberapa menit, untuk menyelesaikan koneksi yang ada dan sedang berlangsung di Availability Zone yang terpengaruh. Untuk informasi selengkapnya, lihat Cara kerja pergeseran zona: pemeriksaan kesehatan dan alamat IP zonal di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.

Pergeseran zona hanya didukung pada Application Load Balancers dan Network Load Balancer dengan penyeimbangan beban lintas zona dimatikan. Jika Anda mengaktifkan penyeimbangan beban lintas zona, Anda tidak dapat memulai pergeseran zona. Untuk informasi selengkapnya, lihat Sumber daya yang didukung untuk pergeseran zona di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.

Sebelum Anda menggunakan pergeseran zona, tinjau hal-hal berikut:

- Penyeimbangan beban lintas zona tidak didukung dengan pergeseran zona. Anda harus mematikan penyeimbangan beban lintas zona untuk menggunakan kemampuan ini.
- Pergeseran zona tidak didukung saat Anda menggunakan Application Load Balancer sebagai titik akhir akselerator di. AWS Global Accelerator
- Anda dapat memulai pergeseran zona untuk penyeimbang beban tertentu hanya untuk satu Availability Zone. Anda tidak dapat memulai pergeseran zona untuk beberapa Availability Zone.
- AWS secara proaktif menghapus alamat IP penyeimbang beban zonal dari DNS ketika beberapa masalah infrastruktur berdampak pada layanan. Selalu periksa kapasitas Availability Zone saat ini sebelum Anda memulai pergeseran zona. Jika penyeimbang beban Anda mematikan penyeimbang beban lintas zona dan Anda menggunakan pergeseran zona untuk menghapus alamat IP penyeimbang beban zonal, Availability Zone yang terpengaruh oleh pergeseran zona juga kehilangan kapasitas target.
- Ketika Application Load Balancer adalah target Network Load Balancer, selalu mulai pergeseran zona dari Network Load Balancer. Jika Anda memulai pergeseran zona dari Application Load Balancer, Network Load Balancer tidak mengenali shift dan terus mengirim lalu lintas ke Application Load Balancer.

Untuk panduan dan informasi selengkapnya, lihat Praktik terbaik dengan pergeseran zona Route 53 ARC di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.

Mulai pergeseran zona

Langkah-langkah dalam prosedur ini menjelaskan cara memulai pergeseran zona menggunakan konsol Amazon EC2. Untuk langkah-langkah memulai pergeseran zona menggunakan konsol Route 53 ARC, lihat Memulai pergeseran zona di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.

Untuk memulai pergeseran 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 nama penyeimbang beban.
4. Pada tab Integrasi, di bawah Route 53 Application Recovery Controller, pilih Mulai pergeseran zona.
5. Pilih Availability Zone yang ingin Anda pindahkan lalu lintas.
6. Pilih atau masukkan kedaluwarsa untuk pergeseran zona. Pergeseran zona awalnya dapat diatur dari 1 menit hingga tiga hari (72 jam).

   Semua pergeseran zona bersifat sementara. Anda harus menetapkan kedaluwarsa, tetapi Anda dapat memperbarui shift aktif nanti untuk menetapkan kedaluwarsa baru.
7. Masukkan komentar. Anda dapat memperbarui pergeseran zona nanti untuk mengedit komentar, jika Anda mau.
8. Pilih kotak centang untuk mengetahui bahwa memulai pergeseran zona akan mengurangi kapasitas aplikasi Anda dengan mengalihkan lalu lintas dari Availability Zone.
9. Pilih Mulai.

Untuk memulai pergeseran zona menggunakan AWS CLI

Untuk bekerja dengan pergeseran zona secara terprogram, lihat Panduan Referensi API Zonal Shift.

Perbarui pergeseran zona

Langkah-langkah dalam prosedur ini menjelaskan cara memperbarui pergeseran zona menggunakan konsol Amazon EC2. Untuk langkah-langkah memperbarui pergeseran zona menggunakan konsol Pengontrol Pemulihan Aplikasi Amazon Route 53, lihat Memperbarui pergeseran zona di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.

Untuk memperbarui pergeseran 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 nama penyeimbang beban yang memiliki pergeseran zona aktif.
4. Pada tab Integrasi, di bawah Route 53 Application Recovery Controller, pilih Perbarui pergeseran zona.

   Ini membuka konsol Route 53 ARC untuk melanjutkan pembaruan.
5. Untuk Mengatur kedaluwarsa pergeseran zona, pilih atau masukkan kedaluwarsa secara opsional.
6. Untuk Komentar, secara opsional edit komentar yang ada atau masukkan komentar baru.
7. Pilih Perbarui.

Untuk memperbarui pergeseran zona menggunakan AWS CLI

Untuk bekerja dengan pergeseran zona secara terprogram, lihat Panduan Referensi API Zonal Shift.

Batalkan pergeseran zona

Langkah-langkah dalam prosedur ini menjelaskan cara membatalkan pergeseran zona menggunakan konsol Amazon EC2. Untuk langkah-langkah membatalkan pergeseran zona menggunakan konsol Pengontrol Pemulihan Aplikasi Amazon Route 53, lihat Membatalkan pergeseran zona di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.

Untuk membatalkan pergeseran 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 nama penyeimbang beban yang memiliki pergeseran zona aktif.
4. Pada tab Integrasi, di bawah Route 53 Application Recovery Controller, pilih Batalkan pergeseran zona.

   Ini membuka konsol Route 53 ARC untuk melanjutkan pembatalan.
5. Pilih Batalkan pergeseran zona.
6. Pada dialog konfirmasi, pilih Konfirmasi.

Untuk membatalkan pergeseran zona menggunakan AWS CLI

Untuk bekerja dengan pergeseran zona secara terprogram, lihat Panduan Referensi API Zonal Shift.

Pendengar untuk Penyeimbang Beban Jaringan Anda

Listener adalah proses yang memeriksa permintaan koneksi, menggunakan protokol dan port yang Anda konfigurasikan. Sebelum Anda mulai menggunakan Network Load Balancer, Anda harus menambahkan setidaknya satu pendengar. Jika penyeimbang beban Anda tidak memiliki pendengar, ia tidak dapat menerima lalu lintas dari klien. Aturan yang Anda tetapkan untuk pendengar menentukan cara penyeimbang beban merutekan permintaan ke target yang Anda daftarkan, seperti instans EC2.

Daftar Isi

Konfigurasi listener

Pendengar mendukung protokol dan port berikut ini:

- Protokol: TCP, TLS, UDP, TCP_UDP
- Port: 1-65535

Anda dapat menggunakan pendengar TLS untuk membongkar karya enkripsi dan dekripsi ke penyeimbang beban Anda sehingga aplikasi Anda dapat fokus pada logika bisnis mereka. Jika protokol pendengar adalah TLS, Anda harus menyebarkan tepat satu sertifikat server SSL pada pendengar. Untuk informasi selengkapnya, lihat Pendengar TLS untuk Penyeimbang Beban Jaringan Anda.

Jika Anda harus memastikan bahwa target mendekripsi lalu lintas TLS alih-alih penyeimbang beban, Anda dapat membuat pendengar TCP di port 443 alih-alih membuat pendengar TLS. Dengan pendengar TCP, penyeimbang beban meneruskan lalu lintas terenkripsi ke target tanpa mendekripsi.

Untuk mendukung TCP dan UDP pada port yang sama, buat pendengar TCP_UDP. Kelompok target untuk pendengar TCP_UDP harus menggunakan protokol TCP_UDP.

Untuk Dualstack Network Load Balancers, hanya protokol TCP dan TLS yang didukung.

Anda dapat menggunakan WebSockets dengan pendengar Anda.

Semua lalu lintas jaringan yang dikirim ke pendengar yang dikonfigurasi diklasifikasikan sebagai lalu lintas yang dimaksudkan. Lalu lintas jaringan yang tidak cocok pendengar yang dikonfigurasi diklasifikasikan sebagai lalu lintas yang tidak diinginkan. Permintaan ICMP selain tipe 3 juga dianggap tidak diinginkan lalu lintas. Penyeimbang Beban Jaringan menjatuhkan lalu lintas yang tidak diinginkan tanpa meneruskannya ke target apa pun. Paket data TCP dikirim ke port pendengar untuk pendengar dikonfigurasi yang tidak koneksi baru atau bagian dari koneksi TCP aktif ditolak dengan reset TCP (RST).

Untuk informasi lebih lanjut, lihat Perutean permintaan di Panduan Pengguna Elastic Load Balancing.

Peraturan listener

Saat membuat pendengar, Anda menentukan aturan untuk merutekan permintaan. Aturan ini meneruskan permintaan ke grup target yang ditentukan. Untuk memperbarui aturan ini, lihat Untuk memperbarui Penyeimbang Beban Jaringan Anda.

Buat pendengar untuk Penyeimbang Beban Jaringan Anda

Suatu pendengar adalah proses yang memeriksa permintaan koneksi. Anda menentukan listener saat membuat penyeimbang beban, dan Anda dapat menambahkan listener ke penyeimbang beban kapan Anda saja.

Prasyarat

- Anda harus menentukan grup target untuk aturan pendengar. Untuk informasi selengkapnya, lihat Buat grup target untuk Penyeimbang Beban Jaringan Anda.
- Anda harus menentukan sertifikat SSL untuk pendengar TLS. Penyeimbang beban menggunakan sertifikat untuk mengakhiri koneksi dan mendekripsi permintaan dari klien sebelum mengarahkan mereka ke target. Untuk informasi selengkapnya, lihat Sertifikat server.

Tambahkan pendengar

Anda mengkonfigurasi pendengar dengan protokol dan port untuk koneksi dari klien untuk penyeimbang beban, dan grup target untuk aturan pendengar default. Untuk informasi selengkapnya, lihat Konfigurasi listener.

Untuk menambahkan pendengar menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Listeners, pilih Add listener.
5. Untuk Protokol, pilih TCP, UDP, TCP_UDP, atau TLS. Menjaga port default atau ketik port yang berbeda. Untuk Dualstack Network Load Balancers, hanya protokol TCP dan TLS yang didukung.
6. Untuk tindakan Default, pilih grup target yang tersedia.
7. [TLS pendengar] Untuk Kebijakan keamanan, kami sarankan Anda menyimpan kebijakan keamanan default.
8. [TLS pendengar] Untuk Sertifikat SSL default, lakukan salah satu langkah berikut:
   - Jika Anda membuat atau mengimpor sertifikat menggunakan AWS Certificate Manager, pilih Dari ACM dan pilih sertifikat.
   - Jika Anda mengunggah sertifikat menggunakan IAM, pilih Dari IAM dan pilih sertifikatnya.
9. [Pendengar TLS] Untuk Kebijakan ALPN, pilih kebijakan untuk mengaktifkan ALPN atau pilih Tidak ada untuk menonaktifkan ALPN. Untuk informasi selengkapnya, lihat Kebijakan ALPN.
10. Pilih Tambahkan.
11. [TLS pendengar] Untuk menambahkan daftar sertifikat opsional untuk digunakan dengan protokol SNI, lihat Menambahkan sertifikat ke daftar sertifikat.

Untuk menambahkan pendengar menggunakan AWS CLI

Penggunaan membuat-pendengar untuk membuat pendengar.

Pendengar TLS untuk Penyeimbang Beban Jaringan Anda

Untuk menggunakan pendengar TLS, Anda harus menyebarkan setidaknya satu sertifikat server pada penyeimbang beban Anda. Penyeimbang beban menggunakan sertifikat server untuk mengakhiri koneksi front-end dan kemudian mendekripsi permintaan dari klien sebelum mengirim mereka ke target. Perhatikan bahwa jika Anda perlu meneruskan lalu lintas terenkripsi ke target tanpa penyeimbang beban mendekripsi, buat pendengar TCP di port 443 alih-alih membuat pendengar TLS. Penyeimbang beban meneruskan permintaan ke target apa adanya, tanpa mendekripsi.

Elastic Load Balancing menggunakan konfigurasi negosiasi TLS, dikenal sebagai kebijakan keamanan, untuk menegosiasikan koneksi TLS antara klien dan penyeimbang beban. Kebijakan keamanan adalah kombinasi dari protokol dan sandi. Protokol membuat koneksi aman antara klien dan server dan memastikan bahwa semua data yang diteruskan antara klien dan penyeimbang beban Anda bersifat pribadi. Sandi adalah algoritme enkripsi yang menggunakan kunci enkripsi untuk membuat pesan kode. Protokol menggunakan beberapa sandi untuk mengenkripsi data melalui internet. Selama proses negosiasi koneksi, klien dan penyeimbang beban menyajikan daftar cipher dan protokol yang masing-masing mendukung, dalam urutan preferensi. Cipher pertama pada daftar server yang cocok salah satu klien cipher dipilih untuk koneksi aman.

Network Load Balancers tidak mendukung negosiasi ulang TLS atau otentikasi TLS bersama (mTLS). Untuk dukungan mTLS, buat pendengar TCP alih-alih pendengar TLS. Penyeimbang beban melewati permintaan apa adanya, sehingga Anda dapat menerapkan mTL pada target.

Untuk membuat pendengar TLS, lihat Tambahkan pendengar. Untuk demo terkait, lihat Support TLS pada Penyeimbang Beban Jaringan dan Support SNI pada Penyeimbang Beban Jaringan.

Sertifikat server

Penyeimbang beban memerlukan sertifikat X.509 (sertifikat server). Sertifikat adalah bentuk digital identifikasi yang dikeluarkan oleh otoritas sertifikat (CA). Sertifikat berisi informasi identifikasi, masa berlaku, kunci publik, nomor seri, dan tanda tangan digital penerbit.

Ketika Anda membuat sertifikat untuk digunakan dengan penyeimbang beban Anda, Anda harus menentukan nama domain. Nama domain pada sertifikat harus cocok dengan catatan nama domain khusus sehingga kami dapat memverifikasi koneksi TLS. Jika mereka tidak cocok, lalu lintas tidak dienkripsi.

Anda harus menentukan nama domain yang sepenuhnya memenuhi syarat (FQDN) untuk sertifikat Anda, seperti `www.example.com` atau nama domain apex seperti. `example.com` Anda juga

dapat menggunakan tanda bintang (*) sebagai kartu liar untuk melindungi beberapa nama situs di domain yang sama. Saat Anda meminta sertifikat kartu liar, tanda bintang (*) harus berada di posisi paling kiri dari nama domain dan hanya dapat melindungi satu tingkat subdomain. Misalnya, `*.example.com` melindungi`corp.example.com`, dan`images.example.com`, tetapi tidak dapat melindungi`test.login.example.com`. Perhatikan juga bahwa `*.example.com` melindungi hanya subdomain dari`example.com`, itu tidak melindungi domain telanjang atau apex (). `example.com` Nama kartu liar muncul di bidang Subjek dan di ekstensi Nama Alternatif Subjek sertifikat. Untuk informasi selengkapnya tentang sertifikat publik, lihat Meminta sertifikat publik di Panduan AWS Certificate Manager Pengguna.

Kami menyarankan Anda membuat sertifikat untuk penyeimbang beban Anda menggunakan AWS Certificate Manager (ACM). ACM terintegrasi dengan Elastic Load Balancing sehingga Anda dapat menyebarkan sertifikat pada penyeimbang beban Anda. Untuk informasi selengkapnya, lihat AWS Certificate Manager Panduan Pengguna.

Atau, Anda dapat menggunakan alat TLS untuk membuat permintaan penandatanganan sertifikat (CSR), lalu mendapatkan CSR yang ditandatangani oleh CA untuk menghasilkan sertifikat, lalu mengimpor sertifikat ke ACM atau mengunggah sertifikat ke (IAM). AWS Identity and Access Management Untuk informasi selengkapnya, lihat Mengimpor sertifikat di Panduan Pengguna AWS Certificate Manager atau Bekerja dengan sertifikat server di Panduan Pengguna IAM.

Daftar Isi

Algoritma kunci yang didukung

- RSA 1024-bit
- RSA 2048-bit
- RSA 3072-bit
- ECDSA 256-bit
- ECDSA 384-bit
- ECDSA 521-bit

Sertifikat default

Bila Anda membuat pendengar TLS, Anda harus menentukan tepat satu sertifikat. Sertifikat ini dikenal sebagai Sertifikat default. Anda dapat mengganti sertifikat default setelah Anda membuat TLS pendengar. Untuk informasi selengkapnya, lihat Ganti sertifikat default.

Jika Anda menentukan sertifikat tambahan di daftar sertifikat, sertifikat default hanya digunakan jika klien tersambung tanpa menggunakan protokol Indikasi Nama Server (SNI) untuk menentukan nama host atau jika tidak ada sertifikat yang cocok dalam daftar sertifikat.

Jika Anda tidak menentukan sertifikat tambahan tetapi perlu menghosting beberapa aplikasi aman melalui penyeimbang beban tunggal, Anda dapat menggunakan sertifikat wildcard atau menambahkan Nama Alternatif Subjek (SAN) untuk setiap domain tambahan ke sertifikat Anda.

Daftar sertifikat

Setelah Anda membuat pendengar TLS, ini memiliki sertifikat default dan daftar sertifikat kosong. Anda dapat menambahkan sertifikat ke daftar sertifikat untuk pendengar. Menggunakan daftar sertifikat memungkinkan penyeimbang beban untuk mendukung beberapa domain pada port yang sama dan memberikan sertifikat yang berbeda untuk setiap domain. Untuk informasi selengkapnya, lihat Menambahkan sertifikat ke daftar sertifikat.

Penyeimbang beban menggunakan algoritme pemilihan sertifikat cerdas dengan dukungan SNI. Jika nama host yang disediakan oleh klien cocok dengan satu sertifikat dalam daftar sertifikat, penyeimbang beban akan memilih sertifikat ini. Jika nama host yang disediakan oleh klien cocok dengan beberapa sertifikat dalam daftar sertifikat, penyeimbang beban memilih sertifikat terbaik yang dapat didukung klien. Pemilihan sertifikat didasarkan pada kriteria dalam urutan sebagai berikut:

- Algoritme hashing (lebih suka SHA daripada MD5)
- Panjang kunci (lebih memilih yang terbesar)
- Masa berlaku

Entri log akses penyeimbang beban menunjukkan nama host yang ditentukan oleh klien dan sertifikat yang diberikan kepada klien. Untuk informasi selengkapnya, lihat Entri akses log.

Perpanjangan sertifikat

Setiap sertifikat memiliki masa berlaku. Anda harus memastikan bahwa Anda memperpanjang atau mengganti setiap sertifikat untuk penyeimbang beban Anda sebelum masa berlakunya berakhir.

Ini termasuk sertifikat default dan sertifikat dalam daftar sertifikat. Memperpanjang atau mengganti sertifikat tidak memengaruhi permintaan dalam penerbangan yang diterima oleh node penyeimbang beban dan sedang menunggu perutean ke target yang sehat. Setelah sertifikat diperpanjang, permintaan baru menggunakan akan menggunakan sertifikat yang telah diperpanjang. Setelah sertifikat diganti, permintaan baru akan menggunakan sertifikat baru.

Anda dapat mengelola perpanjangan sertifikat dan penggantian sebagai berikut:

- Sertifikat yang disediakan oleh AWS Certificate Manager dan digunakan pada penyeimbang beban Anda dapat diperbarui secara otomatis. ACM mencoba untuk memperpanjang sertifikat sebelum masa berlakunya habis. Untuk informasi lebih lanjut, lihat Perpanjangan Terkelola dalam AWS Certificate Manager Panduan Pengguna.
- Jika Anda mengimpor sertifikat ke ACM, Anda harus memantau tanggal kedaluwarsa sertifikat dan memperpanjang masa berlakunya sebelum kedaluwarsa. Untuk informasi lebih lanjut, lihat Mengimpor sertifikat di AWS Certificate Manager Panduan Pengguna.
- Jika Anda mengimpor sertifikat ke IAM, Anda harus membuat sertifikat baru, mengimpor sertifikat baru ke ACM atau IAM, menambahkan sertifikat baru ke penyeimbang beban Anda, dan menghapus sertifikat yang kedaluwarsa dari penyeimbang beban Anda.

Kebijakan Keamanan

Ketika Anda membuat pendengar TLS, Anda harus memilih kebijakan keamanan. Anda dapat memperbarui kebijakan keamanan yang diperlukan. Untuk informasi selengkapnya, lihat Memperbarui kebijakan keamanan.

Pertimbangan:

- `ELBSecurityPolicy-TLS13-1-2-2021-06`Kebijakan ini adalah kebijakan keamanan default untuk pendengar TLS yang dibuat menggunakan. AWS Management Console
  - Kami merekomendasikan kebijakan `ELBSecurityPolicy-TLS13-1-2-2021-06` keamanan, yang mencakup TLS 1.3, dan kompatibel dengan TLS 1.2.
- `ELBSecurityPolicy-2016-08`Kebijakan ini adalah kebijakan keamanan default untuk pendengar TLS yang dibuat menggunakan. AWS CLI
- Anda dapat memilih kebijakan keamanan yang digunakan untuk koneksi front-end, tetapi tidak koneksi backend.

  - Untuk koneksi backend, jika pendengar TLS Anda menggunakan kebijakan keamanan TLS 1.3, kebijakan keamanan akan digunakan. `ELBSecurityPolicy-TLS13-1-0-2021-06` Jika tidak, kebijakan `ELBSecurityPolicy-2016-08` keamanan digunakan untuk koneksi backend.
- Untuk memenuhi standar kepatuhan dan keamanan yang mengharuskan menonaktifkan versi protokol TLS tertentu, atau untuk mendukung klien lama yang membutuhkan cipher usang, Anda dapat menggunakan salah satu kebijakan keamanan. `ELBSecurityPolicy-TLS-` Anda dapat mengaktifkan log akses untuk informasi tentang permintaan TLS yang dikirim ke Network Load Balancer, menganalisis pola lalu lintas TLS, mengelola peningkatan kebijakan keamanan, dan memecahkan masalah. Aktifkan pencatatan akses untuk penyeimbang beban Anda dan periksa entri log akses yang sesuai. Untuk informasi selengkapnya, lihat Access Logs dan Contoh Query Network Load Balancer.
- Anda dapat membatasi kebijakan keamanan mana yang tersedia untuk pengguna di seluruh Anda Akun AWS dan AWS Organizations dengan menggunakan kunci kondisi Elastic Load Balancing di IAM dan kebijakan kontrol layanan (SCP) Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan (SCP) di AWS Organizations Panduan Pengguna

Kebijakan keamanan TLS 1.3

Elastic Load Balancing menyediakan kebijakan keamanan TLS 1.3 berikut untuk Network Load Balancer:

- `ELBSecurityPolicy-TLS13-1-2-2021-06`(Direkomendasikan)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06`
- `ELBSecurityPolicy-TLS13-1-1-2021-06`
- `ELBSecurityPolicy-TLS13-1-0-2021-06`
- `ELBSecurityPolicy-TLS13-1-3-2021-06`

Kebijakan keamanan FIPS

Federal Information Processing Standard (FIPS) adalah standar pemerintah AS dan Kanada yang menetapkan persyaratan keamanan untuk modul kriptografi yang melindungi informasi sensitif. Untuk mempelajari lebih lanjut, lihat Federal Information Processing Standard (FIPS) 140 di halaman Kepatuhan Keamanan AWS Cloud.

Semua kebijakan FIPS memanfaatkan modul kriptografi yang divalidasi AWS-LC FIPS. Untuk mempelajari lebih lanjut, lihat halaman Modul Kriptografi AWS-LC di situs Program Validasi Modul Kriptografi NIST.

Elastic Load Balancing menyediakan kebijakan keamanan FIPS berikut untuk Network Load Balancer:

- `ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`(Direkomendasikan)
- `ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`

Kebijakan yang didukung FS

Elastic Load Balancing menyediakan kebijakan keamanan yang didukung FS (Forward Secrecy) berikut untuk Network Load Balancer:

- `ELBSecurityPolicy-FS-1-2-Res-2020-10`
- `ELBSecurityPolicy-FS-1-2-Res-2019-08`
- `ELBSecurityPolicy-FS-1-2-2019-08`
- `ELBSecurityPolicy-FS-1-1-2019-08`
- `ELBSecurityPolicy-FS-2018-06`

Kebijakan keamanan TLS 1.0 - 1.2

Elastic Load Balancing menyediakan kebijakan keamanan TLS 1.0 - 1.2 berikut untuk Network Load Balancer:

- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-1-2017-01`

- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-TLS-1-0-2015-04`
- `ELBSecurityPolicy-2015-05`(identik dengan **`ELBSecurityPolicy-2016-08`**)

Protokol dan cipher TLS

TLS 1.3

Tabel berikut menjelaskan protokol dan cipher TLS yang didukung untuk kebijakan keamanan TLS 1.3 yang tersedia.

Catatan: `ELBSecurityPolicy-` Awalan telah dihapus dari nama kebijakan di baris kebijakan keamanan.

Contoh: Kebijakan keamanan `ELBSecurityPolicy-TLS13-1-2-2021-06` ditampilkan sebagai`TLS13-1-2-2021-06`.

Kebijakan keamanan	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protokol TLS							
Protocol-TLSv1							✓
Protocol-TLSv1.1						✓	✓
Protocol-TLSv1.2	✓		✓	✓	✓	✓	✓
Protokol-TLSV1.3	✓	✓	✓	✓	✓	✓	✓
Cipher TLS							

Kebijakan keamanan	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓			✓	✓	✓	✓

Kebijakan keamanan	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-RSA-AES128-SHA256	✓			✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓
ECDHE-RSA-AES128-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓			✓	✓	✓	✓

Kebijakan keamanan	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-RSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓
AES128-GCM-SHA256				✓	✓	✓	✓
AES128-SHA256				✓	✓	✓	✓
AES128-SHA				✓		✓	✓
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓

Kebijakan keamanan	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES256-SHA				✓		✓	✓

Untuk membuat pendengar TLS yang menggunakan kebijakan TLS 1.3 menggunakan CLI

Gunakan perintah create-listener dengan kebijakan keamanan TLS 1.3 apa pun.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-TLS13-1-2-2021-06` keamanan.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Untuk memodifikasi pendengar TLS agar menggunakan kebijakan TLS 1.3 menggunakan CLI

Gunakan perintah modify-listener dengan kebijakan keamanan TLS 1.3 apa pun.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-TLS13-1-2-2021-06` keamanan.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Untuk melihat kebijakan keamanan yang digunakan oleh pendengar menggunakan CLI

Gunakan perintah describe-listener dengan listener Anda. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Untuk melihat konfigurasi kebijakan keamanan TLS 1.3 menggunakan CLI

Gunakan describe-ssl-policiesperintah dengan kebijakan keamanan TLS 1.3 apa pun.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-TLS13-1-2-2021-06` keamanan.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

FIPS

> **Important**
>
> Kebijakan `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` dan `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` disediakan hanya untuk kompatibilitas lama. Meskipun mereka menggunakan kriptografi FIPS menggunakan modul FIPS140, mereka mungkin tidak sesuai dengan panduan NIST terbaru untuk konfigurasi TLS.

Tabel berikut menjelaskan protokol dan cipher TLS yang didukung untuk kebijakan keamanan FIPS yang tersedia.

Catatan: `ELBSecurityPolicy-` Awalan telah dihapus dari nama kebijakan di baris kebijakan keamanan.

Contoh: Kebijakan keamanan `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` ditampilkan sebagai`TLS13-1-2-FIPS-2023-04`.

Kebijakan keamanan	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protokol TLS								
Protocol-TLSv1								✓

Kebijakan keamanan	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protocol-TLSv1.1							✓	✓
Protocol-TLSv1.2		✓	✓	✓	✓	✓	✓	✓
Protokol-TLSV1.3	✓	✓	✓	✓	✓	✓	✓	✓
Cipher TLS								
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓

Kebijakan keamanan	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓	✓
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓

Kebijakan keamanan	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-ECDSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384			✓	✓	✓	✓	✓	✓

Kebijakan keamanan	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA256					✓	✓	✓	✓

Kebijakan keamanan	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES256-SHA						✓	✓	✓

Untuk membuat pendengar TLS yang menggunakan kebijakan FIPS menggunakan CLI

Gunakan perintah create-listener dengan kebijakan keamanan FIPS apa pun.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` keamanan.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Untuk memodifikasi pendengar TLS untuk menggunakan kebijakan FIPS menggunakan CLI

Gunakan perintah modify-listener dengan kebijakan keamanan FIPS apa pun.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` keamanan.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Untuk melihat kebijakan keamanan yang digunakan oleh pendengar menggunakan CLI

Gunakan perintah describe-listener dengan listener Anda. `arn`

```
aws elbv2 describe-listener \
```

```
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Untuk melihat konfigurasi kebijakan keamanan FIPS menggunakan CLI

Gunakan describe-ssl-policiesperintah dengan kebijakan keamanan FIPS apa pun.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` keamanan.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

FS

Tabel berikut menjelaskan protokol dan cipher TLS yang didukung untuk kebijakan keamanan yang didukung FS yang tersedia.

Catatan: `ELBSecurityPolicy-` Awalan telah dihapus dari nama kebijakan di baris kebijakan keamanan.

Contoh: Kebijakan keamanan `ELBSecurityPolicy-FS-2018-06` ditampilkan sebagai`FS-2018-06`.

Kebijakan keamanan	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protokol TLS						
Protocol-TLSv1	✓					✓
Protocol-TLSv1.1	✓				✓	✓

Kebijakan keamanan	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
Cipher TLS						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓

Kebijakan keamanan	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-ECDSA-AES128-SHA	✓			✓	✓	✓
ECDHE-RSA-AES128-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓		✓	✓	✓	✓

Kebijakan keamanan	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓			✓	✓	✓
AES128-GCM-SHA256	✓					
AES128-SHA256	✓					
AES128-SHA	✓					
AES256-GCM-SHA384	✓					

Kebijakan keamanan	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-SHA256	✓					
AES256-SHA	✓					

Untuk membuat pendengar TLS yang menggunakan kebijakan yang didukung FS menggunakan CLI

Gunakan perintah create-listener dengan kebijakan keamanan yang didukung FS.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-FS-2018-06` keamanan.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Untuk memodifikasi pendengar TLS agar menggunakan kebijakan yang didukung FS menggunakan CLI

Gunakan perintah modify-listener dengan kebijakan keamanan yang didukung FS.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-FS-2018-06` keamanan.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Untuk melihat kebijakan keamanan yang digunakan oleh pendengar menggunakan CLI

Gunakan perintah describe-listener dengan listener Anda. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Untuk melihat konfigurasi kebijakan keamanan yang didukung FS menggunakan CLI

Gunakan describe-ssl-policiesperintah dengan kebijakan keamanan yang didukung FS.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-FS-2018-06` keamanan.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

TLS 1.0 - 1.2

Tabel berikut menjelaskan protokol dan cipher TLS yang didukung untuk kebijakan keamanan TLS 1.0-1.2 yang tersedia.

Catatan: `ELBSecurityPolicy-` Awalan telah dihapus dari nama kebijakan di baris kebijakan keamanan.

Contoh: Kebijakan keamanan `ELBSecurityPolicy-TLS-1-2-Ext-2018-06` ditampilkan sebagai`TLS-1-2-Ext-2018-06`.

Kebijakan keamanan	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protokol TLS					
Protocol-TLSv1	✓				✓
Protocol-TLSv1.1	✓			✓	✓

Kebijakan keamanan	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocol-TLSv1.2	✓	✓	✓	✓	✓
Cipher TLS					
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	✓		✓	✓
ECDHE-RSA-AES128-SHA	✓	✓		✓	✓

Kebijakan keamanan	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓	✓		✓	✓
ECDHE-ECDSA-AES256-SHA	✓	✓		✓	✓
AES128-GCM-SHA256	✓	✓	✓	✓	✓
AES128-SHA256	✓	✓	✓	✓	✓

Kebijakan keamanan	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
AES128-SHA	✓	✓		✓	✓
AES256-GCM-SHA384	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓
DES-CBC3-SHA					✓

* Jangan gunakan kebijakan ini kecuali Anda harus mendukung klien lama yang memerlukan sandi DES-CBC3-SHA, yang merupakan sandi lemah.

Untuk membuat pendengar TLS yang menggunakan kebijakan TLS 1.0-1.2 menggunakan CLI

Gunakan perintah create-listener dengan kebijakan keamanan yang didukung TLS 1.0-1.2.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-2016-08` keamanan.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Untuk memodifikasi pendengar TLS agar menggunakan kebijakan TLS 1.0-1.2 menggunakan CLI

Gunakan perintah modify-listener dengan kebijakan keamanan yang didukung TLS 1.0-1.2.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-2016-08` keamanan.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Untuk melihat kebijakan keamanan yang digunakan oleh pendengar menggunakan CLI

Gunakan perintah describe-listener dengan listener Anda. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Untuk melihat konfigurasi kebijakan keamanan TLS 1.0-1.2 menggunakan CLI

Gunakan describe-ssl-policiesperintah dengan kebijakan keamanan yang didukung TLS 1.0-1.2.

Contohnya menggunakan kebijakan `ELBSecurityPolicy-2016-08` keamanan.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-2016-08
```

Kebijakan ALPN

Application-Layer Protocol Negotation (ALPN) adalah ekstensi TLS yang dikirim pada pesan hello TLS jabat tangan awal. ALPN memungkinkan lapisan aplikasi untuk menegosiasikan protokol mana yang harus digunakan melalui koneksi aman, seperti HTTP/1 dan HTTP/2.

Ketika klien memulai koneksi ALPN, penyeimbang beban membandingkan daftar preferensi ALPN klien dengan kebijakan ALPN. Jika klien mendukung protokol dari kebijakan ALPN, penyeimbang beban menetapkan sambungan berdasarkan daftar preferensi kebijakan ALPN. Jika tidak, penyeimbang beban tidak menggunakan ALPN.

Kebijakan ALPN yang didukung

Berikut ini adalah kebijakan ALPN yang didukung:

`HTTP1Only`

Negosiasi hanya HTTP/1.*. Daftar preferensi ALPN adalah http/1.1, http/1.0.

`HTTP2Only`

Negosiasi hanya HTTP/2. Daftar preferensi ALPN adalah h2.

`HTTP2Optional`

Lebih suka HTTP/1.* daripada HTTP/2 (yang dapat berguna untuk pengujian HTTP/2). Daftar preferensi ALPN adalah http/1.1, http/1.0, h2.

`HTTP2Preferred`

Lebih suka HTTP/2 daripada HTTP/1.*. Daftar preferensi ALPN adalah h2, http/1.1, http/1.0.

`None`

Jangan bernegosiasi ALPN. Ini adalah pengaturan default.

Aktifkan Koneksi ALPN

Anda dapat mengaktifkan koneksi ALPN ketika Anda membuat atau mengubah pendengar TLS. Untuk informasi lebih lanjut, lihat Tambahkan pendengar dan Memperbarui kebijakan ALPN.

Untuk memperbarui Penyeimbang Beban Jaringan Anda

Anda dapat memperbarui protokol listener, port listener, atau grup target yang menerima lalu lintas dari tindakan penerusan. Tindakan default, juga dikenal sebagai aturan default, meneruskan permintaan ke grup target yang dipilih.

Jika Anda mengubah protokol dari TCP atau UDP ke TLS, Anda harus menentukan kebijakan keamanan dan sertifikat server. Jika Anda mengubah protokol dari TLS ke TCP atau UDP, kebijakan keamanan dan sertifikat server akan dihapus.

Saat grup target untuk tindakan default listener diperbarui, koneksi baru dirutekan ke grup target yang baru dikonfigurasi. Namun, ini tidak berpengaruh pada koneksi aktif apa pun yang dibuat sebelum perubahan ini. Koneksi aktif ini tetap terkait dengan target dalam grup target asli hingga satu jam jika lalu lintas dikirim, atau hingga saat periode idle-timeout berlalu jika tidak ada lalu lintas yang dikirim, mana yang terjadi lebih dulu. Parameter tidak `Connection termination on deregistration`

diterapkan saat memperbarui pendengar, seperti yang diterapkan saat membatalkan pendaftaran target.

Untuk memperbarui pendengar Anda menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Pilih Edit.
6. (Opsional) Ubah nilai yang ditentukan untuk Protokol dan Port sesuai kebutuhan.
7. (Opsional) Pilih grup target yang berbeda untuk tindakan Default.
8. (Opsional) Tambahkan, perbarui, atau hapus tag sesuai kebutuhan.
9. Pilih Simpan perubahan.

Untuk memperbarui pendengar Anda menggunakan AWS CLI

Gunakan perintah ubah-pendengar.

Untuk memperbarui pendengar TLS untuk Penyeimbang Beban Jaringan Anda

Setelah Anda membuat pendengar TLS, Anda dapat mengganti sertifikat default, menambah atau menghapus sertifikat dari daftar sertifikat, memperbarui kebijakan keamanan, atau memperbarui kebijakan ALPN.

Tugas

- Ganti sertifikat default
- Menambahkan sertifikat ke daftar sertifikat
- Menghapus sertifikat dari daftar sertifikat
- Memperbarui kebijakan keamanan
- Memperbarui kebijakan ALPN

Ganti sertifikat default

Anda dapat mengganti sertifikat default untuk pendengar TLS Anda menggunakan prosedur berikut. Untuk informasi selengkapnya, lihat Sertifikat default.

Untuk mengganti sertifikat default menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Untuk Sertifikat SSL default, lakukan salah satu hal berikut:
   - Jika Anda membuat atau mengimpor sertifikat menggunakan AWS Certificate Manager, pilih Dari ACM dan pilih sertifikat.
   - Jika Anda mengunggah sertifikat menggunakan IAM, pilih Dari IAM dan pilih sertifikatnya.
6. Pilih Simpan perubahan.

Untuk mengganti sertifikat default menggunakan AWS CLI

Gunakan perintah ubah-pendengar dengan pilihan --certificates.

Menambahkan sertifikat ke daftar sertifikat

Anda dapat menambahkan sertifikat ke daftar sertifikat untuk pendengar Anda menggunakan prosedur berikut. Ketika Anda pertama kali membuat pendengar TLS, daftar sertifikat kosong. Anda dapat menambahkan satu atau beberapa sertifikat. Anda dapat menambahkan sertifikat default untuk memastikan bahwa sertifikat ini digunakan dengan protokol SNI bahkan jika diganti sebagai sertifikat default. Untuk informasi selengkapnya, lihat Daftar sertifikat.

Untuk menambahkan sertifikat ke daftar sertifikat menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.

4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Pilih kotak centang untuk listener dan pilih Actions, Add SSL certificate for SNI.
6. Untuk menambahkan sertifikat yang sudah dikelola oleh ACM atau IAM, pilih kotak centang untuk sertifikat dan pilih Sertakan sebagai tertunda di bawah ini.
7. Jika Anda memiliki sertifikat yang tidak dikelola oleh ACM atau IAM, pilih Impor sertifikat, lengkapi formulir, dan pilih Impor.
8. Pilih Tambahkan sertifikat yang tertunda.

Untuk menambahkan sertifikat ke daftar sertifikat menggunakan AWS CLI

Gunakan perintah add-listener-certificates.

Menghapus sertifikat dari daftar sertifikat

Anda dapat menghapus sertifikat dari daftar sertifikat untuk pendengar TLS menggunakan prosedur berikut. Untuk menghapus sertifikat default untuk pendengar TLS, lihat Ganti sertifikat default.

Untuk menghapus sertifikat dari daftar sertifikat menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Pilih kotak centang untuk listener dan pilih Actions, Add SSL certificate for SNI.
6. Pilih kotak centang untuk sertifikat dan pilih Hapus.
7. Saat diminta konfirmasi, masukkan **`confirm`** dan pilih Hapus.

Untuk menghapus sertifikat dari daftar sertifikat menggunakan AWS CLI

Gunakan perintah remove-listener-certificates.

Memperbarui kebijakan keamanan

Ketika Anda membuat pendengar TLS, Anda dapat memilih kebijakan keamanan yang memenuhi kebutuhan Anda. Ketika kebijakan keamanan baru ditambahkan, Anda dapat memperbarui

pendengar TLS Anda untuk menggunakan kebijakan keamanan baru. Penyeimbang Beban Jaringan tidak mendukung kebijakan keamanan kustom. Untuk informasi selengkapnya, lihat Kebijakan Keamanan.

Untuk memperbarui kebijakan keamanan menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Pilih Edit.
6. Untuk Kebijakan keamanan, pilih kebijakan keamanan.
7. Pilih Simpan perubahan.

Untuk memperbarui kebijakan keamanan menggunakan AWS CLI

Gunakan perintah ubah-pendengar dengan pilihan --ssl-policy.

Memperbarui kebijakan ALPN

Anda dapat memperbarui kebijakan ALPN untuk pendengar TLS Anda menggunakan prosedur berikut. Untuk informasi selengkapnya, lihat Kebijakan ALPN.

Untuk memperbarui kebijakan ALPN menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Pilih Edit.
6. Untuk Kebijakan ALPN, pilih kebijakan untuk mengaktifkan ALPN atau pilih Tidak ada untuk menonaktifkan ALPN.
7. Pilih Simpan perubahan.

Untuk memperbarui kebijakan ALPN menggunakan AWS CLI

Gunakan perintah ubah-pendengar dengan pilihan --alpn-policy.

Hapus pendengar untuk Penyeimbang Beban Jaringan Anda

Anda dapat menghapus pendengar kapan saja.

Untuk menghapus snapshot menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih kotak centang untuk penyeimbang beban.
4. Pada tab Listeners, pilih kotak centang untuk listener, lalu pilih Actions, Delete listener.
5. Ketika diminta konfirmasi, masukkan **`confirm`** lalu pilih Hapus.

Untuk menghapus pendengar menggunakan AWS CLI

Gunakan perintah hapus-listener.

Target grup untuk Penyeimbang Beban Jaringan 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 grup target yang berbeda untuk berbagai jenis permintaan. Misalnya, membuat satu kelompok target untuk permintaan umum dan kelompok target lain untuk permintaan ke layanan mikro untuk aplikasi Anda. Untuk informasi selengkapnya, lihat Komponen Penyeimbang Beban Jaringan.

Tentukan pengaturan pemeriksaan kesehatan untuk Load Balancer Anda berdasarkan per kelompok 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 kelompok target dalam aturan untuk pendengar, load balancer terus memantau health semua target yang terdaftar dengan kelompok target yang berada di Availability Zone diaktifkan untuk penyeimbang beban. Penyeimbang beban merutekan permintaan untuk target terdaftar yang sehat. Untuk informasi selengkapnya, lihat Pemeriksaan kondisi untuk grup target Anda.

Daftar Isi

- Application Load Balancers sebagai target
- Tag untuk grup target Anda
- Menghapus grup target

Konfigurasi perutean

Secara default, load balancer merutekan permintaan ke targetnya menggunakan protokol dan nomor port yang Anda tentukan saat Anda membuat grup target. Atau, Anda dapat mengganti port yang digunakan untuk merutekan lalu lintas ke target saat Anda mendaftarkannya dengan grup target.

Grup target untuk Penyeimbang Beban Jaringan mendukung protokol dan port berikut:

- Protokol: TCP, TLS, UDP, TCP_UDP
- Port: 1-65535

Jika grup target dikonfigurasi dengan protokol TLS, penyeimbang beban menetapkan koneksi TLS dengan target menggunakan sertifikat yang Anda instal pada target. Penyeimbang beban tidak memvalidasi sertifikat ini. Oleh karena itu, Anda dapat menggunakan sertifikat ditandatangani sendiri atau sertifikat yang telah kedaluwarsa. Karena load balancer berada di virtual private cloud (VPC), lalu lintas antara load balancer dan target diautentikasi pada level paket, sehingga tidak berisiko terkena man-in-the-middle serangan atau spoofing meskipun sertifikat pada target tidak valid.

Tabel berikut merangkum kombinasi yang didukung dari protokol pendengar dan pengaturan grup target.

Protokol pendengar	Protokol grup target	Jenis grup target	Protokol pemeriksaan kondisi
TCP	TCP | TCP_UDP	instans | ip	HTTP | HTTPS | TCP
TCP	TCP	alb	HTTP | HTTPS
TLS	TCP | TLS	instans | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	instans | ip	HTTP | HTTPS | TCP
TCP_UDP	TCP_UDP	instans | ip	HTTP | HTTPS | TCP

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 targetnya.

Status yang mungkin muncul adalah sebagai berikut:

`instance`

Target ditentukan oleh instans ID.

`ip`

Target ditentukan oleh alamat IP.

`alb`

Targetnya adalah Application Load Balancer.

Ketika jenis target`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.

Semua blok CIDR yang didukung memungkinkan Anda untuk mendaftarkan target berikut dengan grup target:

- AWS sumber daya yang dapat dialamatkan oleh alamat IP dan port (misalnya, database).
- Sumber daya lokal yang ditautkan ke AWS melalui AWS Direct Connect atau koneksi VPN Site-to-Site.

Ketika pelestarian IP klien dinonaktifkan untuk grup target Anda, penyeimbang beban dapat mendukung sekitar 55.000 koneksi per menit untuk setiap kombinasi alamat IP Network Load Balancer dan target unik (alamat IP dan port). Jika Anda melebihi koneksi ini, ada kemungkinan peningkatan kesalahan alokasi port. Jika Anda mendapatkan kesalahan alokasi port, tambahkan lebih banyak target ke grup target.

Saat meluncurkan Network Load Balancer di VPC Amazon bersama (sebagai peserta), Anda hanya dapat mendaftarkan target di subnet yang telah dibagikan dengan Anda.

Ketika jenis target adalah`alb`, Anda dapat mendaftarkan Application Load Balancer tunggal sebagai target. Untuk informasi selengkapnya, lihat Application Load Balancers sebagai target.

Penyeimbang Beban Jaringan tidak mendukung jenis target `lambda`. Application Load Balancer adalah satu-satunya penyeimbang beban yang mendukung jenis target `lambda`. Untuk informasi selengkapnya, lihat: Fungsi Lambda sebagai target di Panduan pengguna untuk Application Load Balancers.

Jika Anda memiliki layanan mikro pada instans yang terdaftar dengan Network Load Balancer, Anda tidak dapat menggunakan penyeimbang beban untuk menyediakan komunikasi di antara mereka kecuali penyeimbang beban menghadap ke internet atau instans terdaftar berdasarkan alamat IP. Untuk informasi selengkapnya, lihat Waktu koneksi habis untuk permintaan dari target ke penyeimbang bebannya.

Permintaan perutean dan alamat IP

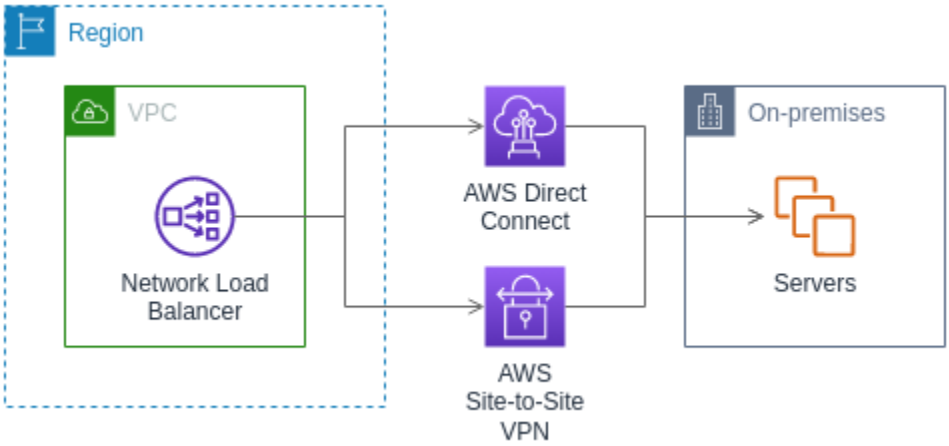
Jika Anda menetapkan target menggunakan ID instans, lalu lintas dialihkan ke instans menggunakan alamat IP privat utama yang ditentukan dalam antarmuka jaringan utama untuk instans. Penyeimbang beban menulis ulang alamat IP tujuan dari paket data sebelum meneruskan ke instans target.

Jika Anda menentukan target menggunakan alamat IP, Anda dapat mengarahkan lalu lintas ke instans menggunakan alamat IP privat dari satu atau beberapa antarmuka jaringan. Hal ini memungkinkan beberapa aplikasi pada instans untuk menggunakan port yang sama. Perhatikan bahwa setiap antarmuka jaringan dapat memiliki grup keamanan sendiri. Penyeimbang beban menulis ulang alamat IP tujuan sebelum meneruskannya ke target.

Untuk informasi selengkapnya tentang mengizinkan lalu lintas ke instans Anda, lihat Menargetkan grup keamanan.

Sumber daya di tempat sebagai target

Sumber daya di tempat yang ditautkan melalui AWS Direct Connect atau koneksi VPN Site-to-Site dapat berfungsi sebagai target, ketika jenis targetnya. `ip`



Saat menggunakan sumber daya di tempat, alamat IP target ini masih harus berasal dari salah satu blok CIDR berikut:

- 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 informasi lebih lanjut tentang AWS Direct Connect, lihat Apa itu AWS Direct Connect?

Untuk informasi lebih lanjut tentang AWS Site-to-Site VPN, lihat Apa itu AWS Site-to-Site VPN?

Jenis alamat IP

Saat membuat grup target baru, Anda dapat memilih jenis alamat IP grup target Anda. Ini mengontrol versi IP yang digunakan untuk berkomunikasi dengan target dan memeriksa status kesehatan mereka.

Network Load Balancers mendukung kelompok sasaran IPv4 dan IPv6. Pilihan default adalah IPv4. Grup target IPv6 hanya dapat dikaitkan dengan Dualstack Network Load Balancers.

Pertimbangan

- Semua alamat IP dalam grup target harus memiliki jenis alamat IP yang sama. Misalnya, Anda tidak dapat mendaftarkan target IPv4 dengan grup target IPv6.
- Grup target IPv6 hanya dapat digunakan dengan penyeimbang `dualstack` beban dengan TCP atau pendengar TLS.
- Kelompok target IPv6 mendukung target tipe IP dan Instance.

Target-target terdaftar.

Penyeimbang beban Anda berfungsi sebagai titik kontak tunggal untuk klien dan mendistribusikan lalu lintas masuk ke target terdaftar yang sehat. Setiap grup target harus memiliki setidaknya satu target yang terdaftar di setiap Availability Zone yang diaktifkan untuk penyeimbang beban. Anda dapat mendaftarkan setiap target dengan satu atau lebih grup target.

Jika permintaan pada aplikasi Anda meningkat, Anda dapat mendaftarkan target tambahan dengan satu atau lebih kelompok target untuk menangani permintaan. Penyeimbang beban mulai merutekan lalu lintas ke target yang baru terdaftar segera setelah proses pendaftaran selesai dan target melewati pemeriksaan kesehatan awal pertama, terlepas dari ambang batas yang dikonfigurasi.

Jika permintaan pada aplikasi Anda menurun, atau jika Anda perlu melayani target Anda, Anda dapat membatalkan pendaftaran target dari grup target Anda. Deregisterasi target menghapus itu dari grup target Anda, tetapi tidak mempengaruhi target sebaliknya. Penyeimbang beban berhenti merutekan lalu lintas ke target segera setelah dibatalkan pendaftarannya. 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.

Jika Anda mendaftarkan target berdasarkan ID instans, Anda dapat menggunakan penyeimbang beban dengan grup Auto Scaling. Setelah Anda melampirkan grup target ke grup Auto Scaling, Auto Scaling akan mendaftarkan target Anda dengan grup target untuk Anda saat meluncurkannya. Untuk informasi selengkapnya, lihat Memasang load balancer ke grup Auto Scaling Anda dalam Amazon EC2 Auto Scaling User Guide.

Persyaratan dan pertimbangan

- Anda tidak dapat mendaftarkan instance berdasarkan ID instans jika menggunakan salah satu jenis instance berikut: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M1, M2, M3, atau T1.

- Saat mendaftarkan target dengan ID instance untuk grup target IPv6, target harus memiliki alamat IPv6 primer yang ditetapkan. Untuk mempelajari lebih lanjut, lihat alamat IPv6 di Panduan Pengguna Amazon EC2
- Saat mendaftarkan target berdasarkan ID instans, instance harus berada dalam VPC Amazon yang sama dengan Network Load Balancer. Anda tidak dapat mendaftarkan instance berdasarkan ID instans jika berada di VPC yang diintip ke VPC penyeimbang beban (Wilayah yang sama atau Wilayah yang berbeda). Anda dapat mendaftarkan instnas ini dengan alamat IP.
- Jika Anda mendaftarkan target dengan alamat IP dan alamat IP berada di VPC yang sama dengan penyeimbang beban, penyeimbang beban memverifikasi bahwa itu adalah dari subnet yang dapat dicapai.
- Penyeimbang beban merutekan lalu lintas ke target hanya di Availability Zone yang diaktifkan. Target di zona yang tidak diaktifkan tidak digunakan.
- Untuk kelompok target UDP dan TCP_UDP, jangan daftarkan instans dengan alamat IP jika mereka berada di luar VPC penyeimbang beban atau jika mereka menggunakan salah satu jenis contoh berikut: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, atau T1. Target yang berada di luar VPC penyeimbang beban atau menggunakan jenis instans yang tidak didukung mungkin dapat menerima lalu lintas dari penyeimbang beban tetapi kemudian tidak dapat merespons.

Atribut grup target

Atribut grup target berikut didukung. Anda dapat memodifikasi atribut ini hanya jika jenis grup target adalah `instance` atau`ip`. Jika tipe grup target adalah`alb`, atribut ini selalu menggunakan nilai defaultnya.

`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.

`deregistration_delay.connection_termination.enabled`

Menunjukkan apakah penyeimbang beban menghentikan koneksi pada akhir batas deregenerasi. Nilainya adalah `true` atau `false`. Untuk grup target UDP/TCP_UDP baru, defaultnya adalah. `true` Jika tidak, default adalah `false`.

`load_balancing.cross_zone.enabled`

Menunjukkan apakah penyeimbangan beban lintas zona diaktifkan. Nilainya adalah`true`, `false` atau`use_load_balancer_configuration`. Default-nya adalah `use_load_balancer_configuration`.

`preserve_client_ip.enabled`

Menunjukkan apakah pelestarian IP klien diaktifkan. Nilainya adalah `true` atau `false`. Default dinonaktifkan jika jenis grup target adalah alamat IP dan protokol grup target adalah TCP atau TLS. Jika tidak, default nya adalah diaktifkan. Pelestarian IP klien tidak dapat dinonaktifkan untuk grup target UDP dan TCP_UDP.

`proxy_protocol_v2.enabled`

Menunjukkan apakah protokol proxy versi 2 diaktifkan. Secara default, protokol proxy dinonaktifkan.

`stickiness.enabled`

Menunjukkan apakah sesi lengket diaktifkan.

`stickiness.type`

Jenis kelengketan. Nilai yang mungkin adalah `source_ip`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

Jumlah minimum target yang harus sehat. Jika jumlah target sehat di bawah nilai ini, tandai zona tersebut sebagai tidak sehat di DNS, sehingga lalu lintas hanya diarahkan ke zona sehat. Nilai yang mungkin adalah`off`, atau bilangan bulat dari 1 ke jumlah maksimum target. Ketika`off`, DNS gagal dinonaktifkan, artinya setiap grup target secara independen berkontribusi pada kegagalan DNS. Default-nya adalah 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

Persentase minimum target yang harus sehat. Jika persentase target sehat di bawah nilai ini, tandai zona sebagai tidak sehat di DNS, sehingga lalu lintas hanya diarahkan ke zona sehat. Nilai yang mungkin adalah`off`, atau bilangan bulat dari 1 hingga 100. Ketika`off`, DNS gagal dinonaktifkan, artinya setiap grup target secara independen berkontribusi pada kegagalan DNS. Default-nya adalah 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

Jumlah minimum target yang harus sehat. Jika jumlah target sehat di bawah nilai ini, kirim lalu lintas ke semua target, termasuk target yang tidak sehat. Kisarannya adalah 1 hingga jumlah target maksimum. Default-nya adalah 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

Persentase minimum target yang harus sehat. Jika persentase target sehat di bawah nilai ini, kirim lalu lintas ke semua target, termasuk target yang tidak sehat. Nilai yang mungkin adalah `off` atau bilangan bulat dari 1 hingga 100. Nilai default-nya `off`.

`target_health_state.unhealthy.connection_termination.enabled`

Menunjukkan apakah penyeimbang beban menghentikan koneksi ke target yang tidak sehat. Nilainya adalah `true` atau `false`. Default adalah `true`.

`target_health_state.unhealthy.draining_interval_seconds`

Jumlah waktu untuk Elastic Load Balancing untuk menunggu sebelum mengubah status target yang tidak sehat dari `unhealthy.draining` ke. `unhealthy` Kisarannya adalah 0-360000 detik. Nilai defaultnya adalah 0 detik.

Catatan: Atribut ini hanya dapat dikonfigurasi ketika `target_health_state.unhealthy.connection_termination.enabledfalse`.

Preservasi IP klien

Network Load Balancers dapat mempertahankan alamat IP sumber klien saat merutekan permintaan ke target backend. Ketika Anda menonaktifkan pelestarian IP klien, alamat IP pribadi Network Load Balancer menjadi alamat IP klien untuk semua lalu lintas yang masuk.

Secara default, pelestarian IP klien diaktifkan (dan tidak dapat dinonaktifkan) misalnya dan grup target tipe IP dengan protokol UDP dan TCP_UDP. Namun, Anda dapat mengaktifkan atau menonaktifkan pelestarian IP klien untuk grup target TCP dan TLS menggunakan atribut grup `preserve_client_ip.enabled` target.

Pengaturan default

- Kelompok target tipe instans: Diaktifkan

- Kelompok target tipe IP (UDP, TCP_UDP): Diaktifkan
- Grup target tipe IP (TCP, TLS): Dinonaktifkan

Persyaratan dan pertimbangan

- Ketika pelestarian IP klien diaktifkan, target harus berada di VPC yang sama dengan Network Load Balancer, dan lalu lintas harus mengalir langsung dari Network Load Balancer ke target.
- Pelestarian IP klien tidak didukung saat menggunakan titik akhir Load Balancer Gateway untuk memeriksa lalu lintas antara Network Load Balancer dan target (instance atau IP), meskipun target berada di Amazon VPC yang sama dengan Network Load Balancer.
- Jenis contoh berikut tidak mendukung pelestarian IP klien: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, dan T1. Kami merekomendasikan bahwa Anda mendaftarkan jenis instans ini sebagai alamat IP dengan pelestarian IP klien dinonaktifkan.
- Pelestarian IP klien tidak berpengaruh pada lalu lintas masuk dari AWS PrivateLink. IP sumber AWS PrivateLink lalu lintas selalu merupakan alamat IP pribadi dari Network Load Balancer.
- Pelestarian IP klien tidak didukung ketika grup target berisi AWS PrivateLink ENI, atau ENI Network Load Balancer lain. Ini akan menyebabkan hilangnya komunikasi dengan target tersebut.
- Pelestarian klien IP tidak berpengaruh pada lalu lintas yang dikonversikan dari IPv6 ke IPv4. IP sumber dari jenis lalu lintas ini selalu merupakan alamat IP privat dari Penyeimbang Beban Jaringan.
- Ketika Anda menentukan target berdasarkan jenis Application Load Balancer, IP klien dari semua lalu lintas yang masuk dipertahankan oleh Network Load Balancer dan dikirim ke Application Load Balancer. Application Load Balancer kemudian menambahkan IP klien ke header `X-Forwarded-For` permintaan sebelum mengirimnya ke target.
- Perubahan pelestarian klien IP berlaku hanya untuk koneksi TCP baru.
- Loopback NAT, juga dikenal sebagai hairpinning, tidak didukung saat pelestarian IP klien diaktifkan. Saat diaktifkan, Anda mungkin mengalami batasan koneksi TCP/IP yang terkait dengan penggunaan kembali soket yang diamati pada target. Keterbatasan sambungan ini dapat terjadi ketika klien, atau perangkat NAT di depan klien, menggunakan alamat IP sumber yang sama dan port sumber saat menghubungkan ke beberapa simpul penyeimbang beban secara bersamaan. Jika penyeimbang beban merutekan koneksi ini ke target yang sama, koneksi muncul ke target seolah-olah mereka berasal dari soket sumber yang sama, yang menghasilkan kesalahan koneksi. Jika hal ini terjadi, klien dapat mencoba lagi (jika sambungan gagal) atau menyambungkan kembali (jika sambungan terganggu). Anda dapat mengurangi jenis kesalahan

koneksi dengan meningkatkan jumlah sumber port fana atau dengan meningkatkan jumlah target untuk penyeimbang beban. Anda dapat mencegah jenis kesalahan koneksi ini, dengan menonaktifkan pelestarian IP klien atau menonaktifkan penyeimbangan beban lintas zona.

- Ketika pelestarian IP klien dinonaktifkan, Network Load Balancer mendukung 55.000 koneksi simultan atau sekitar 55.000 koneksi per menit ke setiap target unik (alamat IP dan port). Jika Anda melebihi koneksi ini, ada kemungkinan peningkatan kesalahan alokasi port, yang mengakibatkan kegagalan untuk membuat koneksi baru. Kesalahan alokasi port dapat dilacak menggunakan metrik. `PortAllocationErrorCount` Untuk memperbaiki kesalahan alokasi port, tambahkan lebih banyak target ke grup target. Untuk informasi selengkapnya, lihat CloudWatch metrik untuk Network Load Balancer.

Untuk mengkonfigurasi pelestarian IP klien 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. Pada tab Atribut, pilih Edit.
5. Untuk mengaktifkan pelestarian IP klien, aktifkan Pertahankan alamat IP klien. Untuk menonaktifkan pelestarian IP klien, matikan Pertahankan alamat IP klien.
6. Pilih Simpan perubahan.

Untuk mengaktifkan atau menonaktifkan pelestarian IP klien menggunakan AWS CLI

Penggunaanmodifikasi-target-kelompok-atributperintah dengan perintah`preserve_client_ip.enabled`atribut.

Misalnya, gunakan perintah berikut untuk menonaktifkan pelestarian IP klien.

```
aws elbv2 modify-target-group-attributes --attributes
 Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

Output Anda harus serupa dengan berikut ini.

```
{
    "Attributes": [
      {
```

```
        "Key": "proxy_protocol_v2.enabled",
        "Value": "false"
      },
      {
        "Key": "preserve_client_ip.enabled",
        "Value": "false"
      },
      {
        "Key": "deregistration_delay.timeout_seconds",
        "Value": "300"
      }
    ]
}
```

Penundaan deregistrasi

Ketika Anda membatalkan pendaftaran target, penyeimbang beban berhenti membuat koneksi baru ke target. Penyeimban beban menggunakan pengosongan koneksi untuk memastikan bahwa lalu lintas dalam penerbangan selesai pada koneksi yang ada. Jika target yang dibatalkan tetap sehat dan sambungan yang ada tidak siaga, penyeimbang beban dapat terus mengirim lalu lintas ke target. Untuk memastikan bahwa koneksi yang ada ditutup, Anda dapat melakukan salah satu dari berikut ini: mengaktifkan atribut grup target untuk penghentian sambungan, memastikan bahwa instans tidak sehat sebelum Anda membatalkan pendaftaran, atau secara berkala menutup sambungan klien.

Keadaan awal dari target yang deregisterasi adalah `draining`. Secara default, penyeimbang beban mengubah keadaan dari target deregisterasi untuk `unused` setelah 300 detik. Untuk mengubah jumlah waktu yang penyeimbang beban tunggu sebelum mengubah keadaan target deregisterasi ke `unused`, perbarui nilai penundaan deregisterasix. Kami sarankan Anda menentukan nilai setidaknya 120 detik untuk memastikan bahwa permintaan selesai.

Jika Anda mengaktifkan atribut grup target untuk penghentian sambungan, koneksi ke target yang dibatalkan ditutup segera setelah akhir batas waktu pembatalan pendaftaran.

Untuk memperbarui atribut 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 target untuk menampilkan detailnya.
4. Pada tab Atribut, pilih Edit.

5. Untuk mengubah batas waktu deregistrasi, masukkan nilai baru untuk Penundaan deregistrasi. Untuk memastikan bahwa koneksi yang ada ditutup setelah Anda membatalkan pendaftaran target, pilih Hentikan koneksi saat deregistrasi.
6. Pilih Simpan perubahan.

Untuk memperbarui atribut deregistrasi menggunakan AWS CLI

Penggunaan perintah ubah-atribut-grup-target.

Protokol proxy

Penyeimbang Beban Jaringan menggunakan protokol proxy versi 2 untuk mengirim informasi koneksi tambahan seperti sumber dan tujuan. Protokol proxy versi 2 menyediakan pengkodean biner dari header protokol proxy. Dengan pendengar TCP, penyeimbang beban menambahkan header protokol proxy ke data TCP. Itu tidak membuang atau menimpa data yang ada, termasuk header protokol proxy yang masuk yang dikirim oleh klien atau proxy lain, penyeimbang beban, atau server di jalur jaringan. Oleh karena itu, dimungkinkan untuk menerima lebih dari satu proxy protokol header. Juga, jika ada jalur jaringan lain ke target Anda di luar Penyeimbang Beban Jaringan, header protokol proxy pertama mungkin bukan yang dari Penyeimbang Beban Jaringan Anda.

Jika Anda menentukan target dengan alamat IP, alamat IP sumber yang disediakan untuk aplikasi Anda tergantung pada protokol grup target sebagai berikut:

- TCP dan TLS: Alamat IP sumber adalah alamat IP privat dari simpul penyeimbang beban. Jika Anda membutuhkan alamat IP klien, aktifkan protokol proxy dan dapatkan alamat IP klien dari header protokol proxy.
- UDP dan TCP_UDP: Alamat IP sumber adalah alamat IP klien.

Jika Anda menentukan target dengan instans ID, alamat IP sumber yang disediakan untuk aplikasi Anda adalah alamat IP klien. Namun, jika Anda lebih suka, Anda dapat mengaktifkan protokol proxy dan mendapatkan alamat IP klien dari header protokol proxy.

> **Note**
>
> Pendengar TLS tidak mendukung koneksi masuk dengan header protokol proxy yang dikirim oleh klien atau proxy lainnya.

Koneksi pemeriksaan kondisi

Setelah Anda mengaktifkan protokol proxy, header protokol proxy juga disertakan dalam sambungan pemeriksaan kondisi dari penyeimbang beban. Namun, dengan sambungan pemeriksaan kondisi, informasi koneksi klien tidak dikirim di header protokol proxy.

Layanan VPC endpoint

Untuk lalu lintas yang berasal dari konsumen layanan melalui Layanan VPC endpoint, alamat IP sumber yang disediakan untuk aplikasi Anda adalah alamat IP privat dari sampul penyeimbang beban. Jika aplikasi Anda membutuhkan alamat IP dari konsumen layanan, aktifkan protokol proxy dan dapatkan layanannya dari header protokol proxy.

Header protokol Proxy juga termasuk ID dari titik akhir. Informasi ini dikodekan menggunakan kustom Type-Length-Value (TLV) vektor sebagai berikut.

Bidang	Panjang (dalam oktet)	Deskripsi
Jenis	1	PP2_TYPE_AWS (0xEA)
Panjang	2	Panjang nilai
Nilai	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	variabel (nilai panjang dikurangi 1)	ID dari titik akhir

Untuk contoh yang menguraikan TLV jenis 0xEA, lihat https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot.

Aktifkan protokol proxy

Sebelum Anda mengaktifkan protokol proxy pada grup target, pastikan bahwa aplikasi Anda mengharapkan dan dapat mengurai header protokol proxy v2, jika tidak, mereka mungkin gagal. Untuk informasi selengkapnya, lihat Protokol Proxy versi 1 dan 2.

Untuk mengaktifkan protokol proxy v2 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 detailnya.
4. Pada tab Atribut, pilih Edit.
5. Pada halaman Edit atribut, pilih Protokol proxy v2.
6. Pilih Simpan perubahan.

Untuk mengaktifkan protokol proxy v2 menggunakan AWS CLI

Gunakan perintah ubah-atribut-grup-target.

Sesi lengket

Sesi lengket adalah mekanisme untuk merutekan lalu lintas klien ke target yang sama dalam grup target. Hal ini berguna untuk server yang mempertahankan informasi negara untuk memberikan pengalaman terus-menerus ke klien.

Pertimbangan

- Menggunakan sesi lengket dapat menyebabkan distribusi koneksi dan aliran yang tidak merata, yang mungkin berdampak pada ketersediaan target Anda. Sebagai contoh, semua klien di belakang perangkat NAT yang sama memiliki alamat IP sumber yang sama. Oleh karena itu, semua lalu lintas dari klien ini diarahkan ke target yang sama.
- Penyeimbang beban dapat mengatur ulang sesi lengket untuk grup target jika status kesehatan salah satu targetnya berubah atau jika Anda mendaftarkan atau membatalkan target dengan grup target.
- Ketika atribut stickiness diaktifkan untuk grup target, pemeriksaan kesehatan pasif tidak didukung. Untuk informasi selengkapnya, lihat Pemeriksaan Kesehatan untuk kelompok sasaran Anda.
- Sesi lengket tidak didukung untuk pendengar TLS.

Untuk mengaktifkan sesi lengket 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. Pada tab Atribut, pilih Edit.

5. Di bawah Konfigurasi pemilihan target, aktifkan Stickiness.
6. Pilih Simpan perubahan.

Untuk mengaktifkan sesi lengket menggunakan AWS CLI

Gunakan perintah ubah-atribut-target-grup dengan atribut `stickiness.enabled`.

Buat grup target untuk Penyeimbang Beban Jaringan Anda

Anda mendaftarkan target untuk Penyeimbang Beban Jaringan Anda dengan grup target. Secara default, penyeimbang beban mengirimkan permintaan ke target yang terdaftar menggunakan port dan protokol yang Anda tentukan untuk grup target. Anda dapat mengganti port ini ketika Anda mendaftar setiap target dengan kelompok target.

Setelah Anda membuat grup target, Anda dapat menambahkan tag.

Untuk merutekan lalu lintas ke target dalam grup target, membuat pendengar dan menentukan kelompok target dalam tindakan default untuk pendengar. Untuk informasi selengkapnya, lihat Peraturan listener. Anda dapat menentukan grup target yang sama di beberapa pendengar, tetapi pendengar ini harus termasuk dalam Network Load Balancer yang sama. Untuk menggunakan grup target dengan penyeimbang beban, Anda harus memverifikasi bahwa grup target tidak digunakan oleh pendengar untuk penyeimbang beban lainnya.

Anda dapat menambah atau menghapus target dari grup target Anda kapan saja. Untuk informasi selengkapnya, lihat Daftarkan target dengan grup target Anda. Anda juga dapat mengubah pengaturan pemeriksaan kesehatan untuk grup target Anda. Untuk informasi selengkapnya, lihat Memodifikasi pengaturan pemeriksaan kondisi dari grup target.

Untuk membuat grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Target Groups.
3. PilihBuat grup target.
4. Untuk panel konfigurasi Dasar, lakukan hal berikut:

    a. Untuk Pilih jenis target, pilih Instans untuk mendaftarkan target berdasarkan ID instans, alamat IP untuk mendaftarkan target berdasarkan alamat IP, atau Application Load Balancer untuk mendaftarkan Application Load Balancer sebagai target.

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. Untuk Protokol, pilih protokol seperti berikut:

- Jika protokol pendengar adalah TCP, pilih TCP atau TCP_UDP.
- Jika protokol pendengar adalah TLS, pilih TCP atau TLS.
- Jika protokol pendengar adalah UDP, pilih UDP atau TCP_UDP.
- Jika protokol pendengar adalah TCP_UDP, pilih TCP_UDP.

d. (Opsional) Untuk Port, mengubah nilai default yang diperlukan.

e. Untuk jenis alamat IP, pilih IPv4 atau IPv6. Opsi ini hanya tersedia jika jenis targetnya adalah Instans atau alamat IP dan protokolnya adalah TCP atau TLS.

   Anda harus mengaitkan grup target IPv6 dengan penyeimbang beban dualstack. Semua target dalam kelompok target harus memiliki jenis alamat IP yang sama. Anda tidak dapat mengubah jenis alamat IP grup target setelah Anda membuatnya.

f. Untuk VPC, pilih virtual private cloud (VPC) dengan target yang akan didaftarkan.

5. Untuk panel Pemeriksaan Kesehatan, ubah pengaturan default sesuai kebutuhan. Untuk Pengaturan pemeriksaan kesehatan tingkat lanjut, pilih port pemeriksaan kesehatan, hitung, waktu habis, interval, dan tentukan kode keberhasilan. 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) Untuk menambahkan tag, perluas Tag, pilih Tambahkan tag, dan masukkan kunci tag dan nilai tag.
7. Pilih Selanjutnya.
8. Pada halaman Daftar target, tambahkan satu atau beberapa target sebagai berikut:
   - Jika jenis targetnya adalah Instans, pilih instance, masukkan port, lalu pilih Sertakan sebagai tertunda di bawah ini.

     Catatan: Instance harus memiliki alamat IPv6 primer yang ditetapkan untuk didaftarkan dengan grup target IPv6.
   - Jika jenis target adalah alamat IP, pilih jaringan, masukkan alamat IP dan port, lalu pilih Sertakan sebagai tertunda di bawah ini.

9. PilihBuat 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. Penyeimbang beban mulai merutekan permintaan ke target yang baru terdaftar segera setelah proses pendaftaran selesai. Diperlukan waktu beberapa menit hingga proses pendaftaran selesai dan pemeriksaan kesehatan dimulai.

Penyeimbang Beban Jaringan menggunakan pemeriksaan kesehatan aktif dan pasif untuk menentukan apakah target tersedia untuk menangani permintaan. Secara default, setiap simpul penyeimbang beban merutekan permintaan hanya untuk target yang sehat di Availability Zone. Jika Anda mengaktifkan penyeimbangan beban lintas zona, setiap simpul penyeimbang beban merutekan permintaan untuk target sehat di semua Availability Zone yang diaktifkan. Untuk informasi selengkapnya, lihat Penyeimbangan beban lintas zona.

Dengan pemeriksaan kesehatan pasif, penyeimbang beban mengamati bagaimana target merespons koneksi. Pemeriksaan kesehatan pasif memungkinkan penyeimbang beban mendeteksi target yang tidak sehat sebelum dilaporkan tidak sehat oleh pemeriksaan kesehatan aktif. Anda tidak dapat menonaktifkan, mengkonfigurasi, atau memantau pemeriksaan kesehatan pasif. Pemeriksaan kesehatan pasif tidak didukung untuk lalu lintas UDP, dan kelompok sasaran dengan lengket dihidupkan. Untuk informasi selengkapnya, lihat Sesi lengket.

Jika target menjadi tidak sehat, penyeimbang beban mengirimkan RST TCP untuk paket yang diterima pada koneksi klien yang terkait dengan target, kecuali target yang tidak sehat memicu penyeimbang beban gagal terbuka.

Jika grup target tidak memiliki target sehat di Availability Zone yang diaktifkan, kami menghapus alamat IP untuk subnet yang sesuai dari DNS sehingga permintaan tidak dapat diarahkan ke target di Zona Ketersediaan. Jika semua target gagal pemeriksaan kesehatan pada saat yang sama di semua Availability Zone diaktifkan, penyeimbang beban gagal terbuka. Network Load Balancers juga akan gagal terbuka ketika Anda memiliki grup target kosong. Efek dari gagal terbuka adalah untuk

mengizinkan lalu lintas ke semua target di semua Availability Zone diaktifkan, terlepas dari status kesehatan mereka.

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.

Untuk permintaan pemeriksaan kesehatan HTTP atau HTTPS, header host berisi alamat IP dari simpul penyeimbang beban dan port pendengar, bukan alamat IP target dan port pemeriksaan kesehatan.

Jika Anda menambahkan pendengar TLS ke Penyeimbang Beban Jaringan Anda, kami melakukan tes konektivitas pendengar. Karena penghentian TLS juga mengakhiri koneksi TCP, koneksi TCP baru dibuat antara penyeimbang beban dan target Anda. Oleh karena itu, Anda mungkin melihat koneksi TCP untuk pengujian ini dikirim dari penyeimbang beban Anda ke target yang terdaftar dengan pendengar TLS Anda. Anda dapat mengidentifikasi koneksi TCP ini karena mereka memiliki alamat IP sumber Network Load Balancer Anda dan koneksi tidak berisi paket data.

Untuk layanan UDP, ketersediaan target dapat diuji menggunakan pemeriksaan kesehatan non-UDP pada grup target Anda. Anda dapat menggunakan pemeriksaan kesehatan yang tersedia (TCP, HTTP, atau HTTPS), dan setiap port pada target Anda untuk memverifikasi ketersediaan layanan UDP. Jika layanan yang menerima pemeriksaan kesehatan gagal, target Anda dianggap tidak tersedia. Untuk meningkatkan akurasi pemeriksaan kesehatan untuk layanan UDP, mengkonfigurasi layanan mendengarkan port pemeriksaan kesehatan untuk melacak status layanan UDP Anda dan gagal pemeriksaan kesehatan jika layanan tidak tersedia.

Pengaturan pemeriksaan kesehatan

Anda mengkonfigurasi pemeriksaan kesehatan aktif untuk target dalam grup target menggunakan pengaturan berikut. Jika pemeriksaan kesehatan melebihi UnhealthyThresholdHitung kegagalan berturut-turut, penyeimbang beban mengeluarkan target dari layanan. Ketika pemeriksaan kesehatan melebihi HealthyThresholdHitungan keberhasilan berturut-turut, penyeimbang beban menempatkan target kembali dalam layanan.

Pengaturan	Deskripsi	Default
HealthCheckProtokol	Protokol penyeimbang beban gunakan saat melakukan pemeriksaan kesehatan pada target. Protokol yang mungkin adalah	TCP

Pengaturan	Deskripsi	Default
	HTTP, HTTPS, dan TCP. Default-nya adalah protokol TCP. Jika jenis targetnya`alb`, protokol pemeriksaan kesehatan yang didukung adalah HTTP dan HTTPS.	
HealthCheckPelabuhan	Port penyeimbang beban digunakan saat melakukan pemeriksaan kondisi pada target. Defaultnya adalah dengan menggunakan port di mana setiap target menerima lalu lintas dari penyeimbang beban.	Port di mana setiap target menerima lalu lintas dari penyeimba ng beban.
HealthCheckJalan	[Pemeriksaan kesehatan HTTP/HTTPS] Jalur pemeriksaan kesehatan yang menjadi tujuan pada target pemeriksaan kesehatan. Default-n ya adalah /.	/
HealthCheckTimeoutSeconds	Jumlah waktu, dalam detik, di mana tidak ada respons dari target berarti pemeriksaan kondisi gagal. Rentangnya adalah 2–120 detik. Nilai default adalah 6 detik untuk HTTP dan 10 detik untuk pemeriksaan kesehatan TCP dan HTTPS.	6 detik untuk pemeriksaan kesehatan HTTP dan 10 detik untuk pemeriksaan kesehatan TCP dan HTTPS.

Pengaturan	Deskripsi	Default
HealthCheckIntervalSeconds	Perkiraan jumlah waktu, dalam hitungan detik, antara pemeriksaan kondisi dari target individu. Rentangnya adalah 5-300 detik. Waktu default-nya adalah 30 detik. **Important** Pemeriksaan Kesehatan untuk Penyeimbang Beban Jaringan didistrib usikan dan menggunakan mekanisme konsensus untuk menentukan target kesehatan. Oleh karena itu, target menerima lebih dari jumlah dikonfigu rasi pemeriksaan kesehatan. Untuk mengurangi dampak target Anda jika Anda menggunakan pemeriksaan kesehatan HTTP, gunakan tujuan sederhana pada target, seperti file HTML statis, atau beralih ke pemeriksa an kesehatan TCP.	30 detik
HealthyThresholdHitung	Jumlah pemeriksaan kondisi yang berhasil berturut-turut diperlukan sebelum menganggap target yang tidak sehat memiliki kondisi sehat. Rentangnya adalah 2–10. Defaultnya adalah 5.	5
UnhealthyThresholdHitung	Jumlah pemeriksaan kondisi yang gagal berturut-turut diperlukan sebelum mengangga p target yang tidak memiliki kondisi sehat. Rentangnya adalah 2–10. Defaultnya adalah 2.	2

Pengaturan	Deskripsi	Default
Matcher	[Pemeriksaan kesehatan HTTP/HTTPS] Kode HTTP yang digunakan saat memeriksa respons yang berhasil dari target. Kisaranny a adalah 200 hingga 599. Defaultnya adalah 200-399.	200-399

Status kondisi target

Sebelum penyeimbang beban mengirimkan permintaan pemeriksaan kesehatan ke target, Anda harus mendaftarkannya dengan grup target, menentukan grup targetnya dalam aturan pendengar, dan memastikan bahwa Availability Zone target diaktifkan untuk penyeimbang beban.

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

Nilai	Deskripsi
`initial`	Penyeimbang beban sedang dalam proses mendaftarkan target atau melakukan pemeriksaan kondisi awal pada target. Kode alasan terkait: `Elb.RegistrationIn Progress` | `Elb.InitialHealthChecking`
`healthy`	Targetnya sehat. Kode alasan terkait: Tidak ada
`unhealthy`	Target tidak menanggapi pemeriksaan kesehatan, gagal pemeriksaan kesehatan, atau target dalam keadaan berhenti. Kode alasan terkait: `Target.FailedHealthChecks`
`draining`	Target membatalkan pendaftaran dan pengosongan koneksi sedang dalam proses.

Nilai	Deskripsi
	Kode alasan terkait: `Target.DeregistrationInProgress`
`unhealthy.draining`	Target tidak menanggapi pemeriksaan kesehatan atau gagal dalam pemeriksaan kesehatan dan memasuki masa tenggang. Target mendukung koneksi yang ada dan tidak akan menerima koneksi baru selama masa tenggang ini. Kode alasan terkait: `Target.FailedHealthChecks`
`unavailable`	Target kesehatan tidak tersedia. Kode alasan terkait: `Elb.InternalError`
`unused`	Target tidak terdaftar dengan grup target, grup target tidak digunakan dalam aturan listener, atau target berada di Availability Zone yang tidak diaktifkan. Kode alasan terkait: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`

Kode alasan pemeriksaan kondisi

Jika status target adalah nilai selain `Healthy`, API mengembalikan kode alasan dan deskripsi masalah, dan konsol menampilkan deskripsi yang sama di tooltip. Perhatikan bahwa kode alasan yang dimulai dengan `Elb` berasal dari sisi penyeimbang beban dan kode alasan yang dimulai dengan `Target` berasal dari sisi target.

Kode alasan	Deskripsi
`Elb.InitialHealthChecking`	Pemeriksaan kondisi awal sedang berlangsung
`Elb.InternalError`	Pemeriksaan kondisi gagal karena kesalahan internal

Kode alasan	Deskripsi
`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 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 penyeimbang beban Target berada di Availability Zone yang tidak diaktifkan untuk penyeimbang beban
`Target.NotRegistered`	Target tidak terdaftar ke grup target

Periksa kesehatan 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. Panel Detail menampilkan jumlah total target, ditambah jumlah target untuk setiap status kesehatan.
5. Pada tab Target, kolom Status Kesehatan menunjukkan status setiap target.
6. Jika status target adalah nilai apa pun selain`Healthy`, kolom Detail status Kesehatan berisi informasi lebih lanjut.

Untuk memeriksa kesehatan target Anda menggunakan AWS CLI

Gunakan perintah jelaskan-kondisi-target. 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.

Memodifikasi pengaturan pemeriksaan kondisi dari grup target

Anda dapat mengubah pengaturan pemeriksaan kondisi untuk grup target kapan saja.

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 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 modifikasi-grup-target.

Penyeimbangan beban lintas zona untuk kelompok sasaran

Node untuk Load Balancer Anda mendistribusikan permintaan dari klien ke target yang telah terdaftar. Saat penyeimbangan beban lintas zona aktif, setiap node penyeimbang beban

mendistribusikan lalu lintas ke seluruh target terdaftar di semua Availability Zone yang terdaftar. Ketika penyeimbangan beban lintas zona tidak aktif, setiap node penyeimbang beban mendistribusikan lalu lintas hanya di target terdaftar di Availability Zone. Ini dapat digunakan jika domain kegagalan zona lebih disukai daripada regional, memastikan bahwa zona sehat tidak terpengaruh oleh zona yang tidak sehat, atau untuk peningkatan latensi secara keseluruhan.

Dengan Network Load Balancers, penyeimbangan beban lintas zona dinonaktifkan secara default di tingkat penyeimbang beban, tetapi Anda dapat menyalakannya kapan saja. Untuk grup target, defaultnya adalah menggunakan pengaturan penyeimbang beban, tetapi Anda dapat mengganti default dengan mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona secara eksplisit di tingkat grup target.

Pertimbangan

- Saat mengaktifkan penyeimbangan beban lintas zona untuk Network Load Balancer, biaya transfer data EC2 berlaku. Untuk informasi selengkapnya, lihat Memahami biaya transfer AWS data di Panduan Pengguna Ekspor Data
- Pengaturan grup target menentukan perilaku load balancing untuk kelompok target. Misalnya, jika penyeimbangan beban lintas zona diaktifkan pada tingkat penyeimbang beban dan dinonaktifkan pada tingkat grup target, lalu lintas yang dikirim ke grup target tidak dirutekan melintasi Availability Zone.
- Saat penyeimbangan beban lintas zona mati, pastikan Anda memiliki kapasitas target yang cukup di setiap Zona Ketersediaan penyeimbang beban, sehingga setiap zona dapat melayani beban kerja yang terkait.
- Ketika penyeimbangan beban lintas zona tidak aktif, pastikan bahwa semua kelompok target berpartisipasi dalam Availability Zone yang sama. Availability Zone yang kosong dianggap tidak sehat.

Memodifikasi penyeimbangan beban lintas zona untuk penyeimbang beban

Anda dapat mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona pada tingkat penyeimbang beban kapan saja.

Untuk memodifikasi penyeimbangan beban lintas zona untuk penyeimbang beban 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 nama penyeimbang beban untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Pada halaman Edit atribut penyeimbang beban, aktifkan atau nonaktifkan penyeimbangan beban lintas zona.
6. Pilih Simpan perubahan.

Untuk memodifikasi penyeimbangan beban lintas zona untuk penyeimbang beban Anda menggunakan AWS CLI

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

Memodifikasi penyeimbangan beban lintas zona untuk grup target

Pengaturan penyeimbangan beban lintas zona pada tingkat kelompok target mengesampingkan pengaturan di tingkat penyeimbang beban.

Anda dapat mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona di tingkat grup target jika tipe grup target adalah `instance` atau. `ip` Jika tipe grup target adalah`alb`, grup target selalu mewarisi pengaturan penyeimbangan beban lintas zona dari penyeimbang beban.

Untuk memodifikasi penyeimbangan beban lintas zona untuk grup target menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Load Balancing, pilih Grup Target.
3. Pilih nama grup target untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Pada halaman Edit atribut grup target, pilih Aktif untuk penyeimbangan beban lintas zona.
6. Pilih Simpan perubahan.

Untuk memodifikasi penyeimbangan beban lintas zona untuk grup target menggunakan AWS CLI

Penggunaanmodifikasi-target-kelompok-atributperintah dengan perintah`load_balancing.cross_zone.enabled`atribut.

Kesehatan kelompok sasaran

Secara default, kelompok sasaran dianggap sehat selama memiliki setidaknya satu target yang sehat. Jika Anda memiliki armada besar, hanya memiliki satu target yang sehat yang melayani lalu lintas tidak cukup. Sebagai gantinya, Anda dapat menentukan jumlah minimum atau persentase target yang harus sehat, dan tindakan apa yang dilakukan penyeimbang beban ketika target sehat jatuh di bawah ambang batas yang ditentukan. Ini meningkatkan ketersediaan.

Tindakan negara yang tidak sehat

Anda dapat mengonfigurasi ambang batas yang sehat untuk tindakan berikut:

- DNS failover — Ketika target sehat di zona jatuh di bawah ambang batas, kami menandai alamat IP node penyeimbang beban untuk zona sebagai tidak sehat di DNS. Oleh karena itu, ketika klien menyelesaikan nama DNS penyeimbang beban, lalu lintas dialihkan hanya ke zona sehat.
- Routing failover — Ketika target sehat di zona jatuh di bawah ambang batas, penyeimbang beban mengirimkan lalu lintas ke semua target yang tersedia untuk node penyeimbang beban, termasuk target yang tidak sehat. Hal ini meningkatkan kemungkinan koneksi klien berhasil, terutama ketika target sementara gagal lulus pemeriksaan kesehatan, dan mengurangi risiko kelebihan beban target yang sehat.

Persyaratan dan pertimbangan

- Jika Anda menentukan kedua jenis ambang batas untuk suatu tindakan (hitungan dan persentase), penyeimbang beban akan mengambil tindakan ketika salah satu ambang batas dilanggar.
- Jika Anda menentukan ambang batas untuk kedua tindakan, ambang batas untuk failover DNS harus lebih besar dari atau sama dengan ambang batas untuk routing failover, sehingga failover DNS terjadi baik dengan atau sebelum routing failover.
- Jika Anda menentukan ambang batas sebagai persentase, kami menghitung nilai secara dinamis, berdasarkan jumlah total target yang terdaftar dengan kelompok target.
- Jumlah total target didasarkan pada apakah penyeimbangan beban lintas zona mati atau aktif. Jika penyeimbangan beban lintas zona tidak aktif, setiap node mengirimkan lalu lintas hanya ke target di zonanya sendiri, yang berarti bahwa ambang batas berlaku untuk jumlah target di setiap zona yang diaktifkan secara terpisah. Jika penyeimbangan beban lintas zona aktif, setiap node mengirimkan lalu lintas ke semua target di semua zona yang diaktifkan, yang berarti bahwa

ambang batas yang ditentukan berlaku untuk target jumlah total di semua zona yang diaktifkan. Untuk informasi selengkapnya, lihat Penyeimbangan beban lintas zona.

- Dengan failover DNS, kami menghapus alamat IP untuk zona tidak sehat dari nama host DNS untuk penyeimbang beban. Namun, cache DNS klien lokal mungkin berisi alamat IP ini sampai time-to-live (TTL) dalam catatan DNS berakhir (60 detik).
- Ketika failover DNS terjadi, ini berdampak pada semua kelompok target yang terkait dengan penyeimbang beban. Pastikan Anda memiliki kapasitas yang cukup di zona yang tersisa untuk menangani lalu lintas tambahan ini, terutama jika penyeimbangan beban lintas zona tidak aktif.
- Dengan failover DNS, jika semua zona penyeimbang beban dianggap tidak sehat, penyeimbang beban mengirimkan lalu lintas ke semua zona, termasuk zona yang tidak sehat.
- Ada faktor selain apakah ada target sehat yang cukup yang dapat menyebabkan kegagalan DNS, seperti kesehatan zona.

Contoh

Contoh berikut menunjukkan bagaimana pengaturan kesehatan kelompok target diterapkan.

Skenario

- Penyeimbang beban yang mendukung dua Availability Zone, A dan B
- Setiap Availability Zone berisi 10 target terdaftar
- Kelompok sasaran memiliki pengaturan kesehatan kelompok sasaran berikut:
  - DNS failover - 50%
  - Failover perutean - 50%
- Enam target gagal di Availability Zone B

Jika penyeimbangan beban lintas zona tidak aktif

- Node penyeimbang beban di setiap Availability Zone hanya dapat mengirim lalu lintas ke 10 target di Availability Zone.
- Ada 10 target sehat di Availability Zone A, yang memenuhi persentase target sehat yang diperlukan. Load balancer terus mendistribusikan lalu lintas antara 10 target sehat.
- Hanya ada 4 target sehat di Availability Zone B, yaitu 40% dari target untuk node penyeimbang beban di Availability Zone B. Karena ini kurang dari persentase target sehat yang dibutuhkan, penyeimbang beban mengambil tindakan berikut:

- DNS failover - Availability Zone B ditandai sebagai tidak sehat di DNS. Karena klien tidak dapat menyelesaikan nama penyeimbang beban ke node penyeimbang beban di Availability Zone B, dan Availability Zone A sehat, klien mengirim koneksi baru ke Availability Zone A.
- Routing failover - Ketika koneksi baru dikirim secara eksplisit ke Availability Zone B, load balancer mendistribusikan lalu lintas ke semua target di Availability Zone B, termasuk target yang tidak sehat. Ini mencegah pemadaman di antara target sehat yang tersisa.

Jika penyeimbangan beban lintas zona aktif

- Setiap node penyeimbang beban dapat mengirim lalu lintas ke semua 20 target terdaftar di kedua Availability Zone.
- Ada 10 target sehat di Availability Zone A dan 4 target sehat di Availability Zone B, dengan total 14 target sehat. Ini adalah 70% dari target untuk node penyeimbang beban di kedua Availability Zone, yang memenuhi persentase target sehat yang diperlukan.
- Penyeimbang beban mendistribusikan lalu lintas antara 14 target sehat di kedua Availability Zone.

Ubah pengaturan kesehatan kelompok sasaran

Anda dapat memodifikasi pengaturan kesehatan grup target untuk grup target Anda sebagai berikut.

Untuk mengubah pengaturan kesehatan 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 Atribut, pilih Edit.
5. Periksa apakah penyeimbangan beban lintas zona dihidupkan atau dimatikan. Perbarui pengaturan ini sesuai kebutuhan untuk memastikan bahwa Anda memiliki kapasitas yang cukup untuk menangani lalu lintas tambahan jika zona gagal.
6. Perluas persyaratan kesehatan kelompok sasaran.
7. Untuk jenis Konfigurasi, sebaiknya pilih Konfigurasi terpadu, yang menetapkan ambang batas yang sama untuk kedua tindakan tersebut.
8. Untuk persyaratan keadaan Sehat, lakukan salah satu hal berikut:
    - Pilih Jumlah target sehat minimum, lalu masukkan angka dari 1 hingga jumlah target maksimum untuk kelompok target Anda.

- Pilih Persentase target sehat minimum, lalu masukkan angka dari 1 hingga 100.

9. Pilih Simpan perubahan.

Untuk memodifikasi pengaturan kesehatan kelompok target menggunakan AWS CLI

Penggunaan perintah ubah-atribut-grup-target. Contoh berikut menetapkan ambang batas yang sehat untuk kedua tindakan negara yang tidak sehat menjadi 50%.

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

Pengakhiran koneksi untuk target yang tidak sehat

Penghentian koneksi diaktifkan secara default. Ketika target Network Load Balancer gagal dalam pemeriksaan kesehatan yang dikonfigurasi dan dianggap tidak sehat, penyeimbang beban menghentikan koneksi yang sudah ada dan berhenti merutekan koneksi baru ke target. Dengan penghentian koneksi dinonaktifkan target masih dianggap tidak sehat dan tidak akan menerima koneksi baru, tetapi koneksi yang sudah mapan tetap aktif, memungkinkan mereka untuk menutup dengan anggun.

Pengakhiran koneksi untuk target yang tidak sehat dapat ditetapkan secara individual untuk setiap kelompok sasaran.

Untuk mengubah pengaturan penghentian koneksi 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 Atribut, pilih Edit.
5. Di bawah Target manajemen status tidak sehat, pilih apakah Hentikan koneksi saat target menjadi tidak sehat diaktifkan atau dinonaktifkan.
6. Pilih Simpan perubahan.

Untuk mengubah setelan penghentian koneksi menggunakan AWS CLI

Penggunaanmodifikasi-target-kelompok-atributperintah dengan perintah`target_health_state.unhealthy.connection_termination.enabled`atribut.

Interval pengeringan yang tidak sehat

> **Important**
>
> Penghentian koneksi harus dinonaktifkan sebelum mengaktifkan interval pengeringan yang tidak sehat.

Target di `unhealthy.draining` negara bagian dianggap tidak sehat, tidak menerima koneksi baru, tetapi mempertahankan koneksi yang ditetapkan untuk interval yang dikonfigurasi. Interval koneksi yang tidak sehat menentukan jumlah waktu target tetap dalam `unhealthy.draining` keadaan sebelum keadaannya menjadi`unhealthy`. Jika target melewati pemeriksaan kesehatan selama interval koneksi yang tidak sehat, keadaannya menjadi `healthy` lagi. Jika deregistrasi dipicu, status target menjadi `draining` dan batas waktu tunda deregistrasi dimulai.

Interval pengeringan yang tidak sehat dapat diatur secara individual untuk setiap kelompok sasaran.

Untuk memodifikasi interval pengeringan yang tidak sehat 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 Atribut, pilih Edit.
5. Di bawah Target manajemen status yang tidak sehat, pastikan Hentikan koneksi ketika target menjadi tidak sehat dimatikan.
6. Masukkan nilai untuk Interval pengeringan yang tidak sehat.
7. Pilih Simpan perubahan.

Untuk memodifikasi interval pengeringan yang tidak sehat menggunakan AWS CLI

Penggunaanmodifikasi-target-kelompok-atributperintah dengan perintah`target_health_state.unhealthy.draining_interval_seconds`atribut.

Menggunakan failover DNS Route 53 untuk penyeimbang beban Anda

Jika Anda menggunakan Route 53 untuk merutekan kueri DNS ke penyeimbang beban, Anda juga dapat mengonfigurasi failover DNS untuk penyeimbang beban menggunakan Route 53. Dalam konfigurasi failover, Route 53 memeriksa kesehatan target kelompok target untuk penyeimbang beban untuk menentukan apakah target tersebut tersedia. Jika tidak ada target sehat yang terdaftar di penyeimbang beban, atau jika penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan lalu lintas ke sumber daya lain yang tersedia, seperti penyeimbang beban yang sehat atau situs web statis di Amazon S3.

Misalnya, misalkan Anda memiliki aplikasi web untuk`www.example.com`, dan Anda ingin instance redundan berjalan di belakang dua penyeimbang beban yang berada di Wilayah yang berbeda. Anda ingin lalu lintas terutama diarahkan ke penyeimbang beban di satu Wilayah, dan Anda ingin menggunakan penyeimbang beban di Wilayah lain sebagai cadangan selama kegagalan. Jika Anda mengonfigurasi failover DNS, Anda dapat menentukan penyeimbang beban primer dan sekunder (cadangan) Anda. Rute 53 mengarahkan lalu lintas ke penyeimbang beban utama jika tersedia, atau ke penyeimbang beban sekunder sebaliknya.

Menggunakan evaluasi kesehatan target

- Ketika mengevaluasi kesehatan target diatur ke `Yes` catatan alias untuk Network Load Balancer, Route 53 mengevaluasi kesehatan sumber daya yang ditentukan oleh nilai. `alias target` Untuk Network Load Balancer, Route 53 menggunakan pemeriksaan kesehatan kelompok sasaran yang terkait dengan penyeimbang beban.
- Ketika semua kelompok sasaran dalam Network Load Balancer sehat, Route 53 menandai catatan alias sebagai sehat. Jika kelompok sasaran berisi setidaknya satu target sehat, pemeriksaan kesehatan kelompok sasaran lolos. Route 53 kemudian mengembalikan catatan sesuai dengan kebijakan perutean Anda. Jika kebijakan routing failover digunakan, Route 53 mengembalikan catatan utama.
- Jika salah satu grup target dalam Network Load Balancer tidak sehat, catatan alias gagal dalam pemeriksaan kesehatan Route 53 (fail-open). Jika menggunakan evaluasi kesehatan target, ini akan gagal dalam kebijakan perutean failover.
- Jika semua grup target dalam Network Load Balancer kosong (tidak ada target), maka Route 53 menganggap catatan tidak sehat (fail-open). Jika menggunakan evaluasi kesehatan target, ini akan gagal dalam kebijakan perutean failover.

Untuk informasi selengkapnya, lihat Mengonfigurasi failover DNS di Panduan Pengembang Amazon Route 53.

Daftarkan target dengan grup target Anda

Ketika target Anda siap untuk menangani permintaan, Anda mendaftarkannya dengan satu atau lebih kelompok target. Jenis target dari kelompok target menentukan bagaimana Anda mendaftarkan target. Misalnya, Anda dapat mendaftarkan ID instans, alamat IP, atau Application Load Balancer. Network Load Balancer Anda mulai merutekan permintaan ke target segera setelah proses pendaftaran selesai dan target lulus 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 untuk proses deregistrasi selesai dan penyeimbang beban untuk 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 deregistrasi.

Jika Anda mendaftarkan target berdasarkan ID instans, Anda dapat menggunakan penyeimbang beban dengan grup Auto Scaling. Setelah Anda melampirkan grup target ke grup Auto Scaling dan grup skala keluar, instans yang diluncurkan oleh grup Auto Scaling secara otomatis terdaftar dengan grup target. Jika Anda memisahkan penyeimbang beban dari grup Auto Scaling, maka instans tersebut dikeluarkan secara otomatis dari grup target. Untuk Informasi Selengkapnya, Lihat Memasang load balancer to your Auto Scaling group pada Amazon EC2 Auto Scaling User Guide.

Menargetkan grup keamanan

Sebelum menambahkan target ke grup target Anda, konfigurasikan grup keamanan yang terkait dengan target untuk menerima lalu lintas dari Network Load Balancer Anda.

Rekomendasi untuk kelompok keamanan target jika penyeimbang beban memiliki grup keamanan terkait

- Untuk mengizinkan lalu lintas klien: Tambahkan aturan yang mereferensikan grup keamanan yang terkait dengan penyeimbang beban.
- Untuk mengizinkan PrivateLink lalu lintas: Jika Anda mengonfigurasi penyeimbang beban untuk mengevaluasi aturan masuk untuk lalu lintas yang dikirim AWS PrivateLink, tambahkan aturan yang menerima lalu lintas dari grup keamanan penyeimbang beban di port lalu lintas. Jika tidak, tambahkan aturan yang menerima lalu lintas dari alamat IP pribadi penyeimbang beban di port lalu lintas.
- Untuk menerima pemeriksaan kesehatan penyeimbang beban: Tambahkan aturan yang menerima lalu lintas pemeriksaan kesehatan dari grup keamanan penyeimbang beban di port pemeriksaan kesehatan.

Rekomendasi untuk kelompok keamanan target jika penyeimbang beban tidak terkait dengan grup keamanan

- Untuk mengizinkan lalu lintas klien: Jika penyeimbang beban Anda mempertahankan alamat IP klien, tambahkan aturan yang menerima lalu lintas dari alamat IP klien yang disetujui di port lalu lintas. Jika tidak, tambahkan aturan yang menerima lalu lintas dari alamat IP pribadi penyeimbang beban di port lalu lintas.
- Untuk mengizinkan PrivateLink lalu lintas: Tambahkan aturan yang menerima lalu lintas dari alamat IP pribadi penyeimbang beban di port lalu lintas.
- Untuk menerima pemeriksaan kesehatan penyeimbang beban: Tambahkan aturan yang menerima lalu lintas pemeriksaan kesehatan dari alamat IP pribadi penyeimbang beban di port pemeriksaan kesehatan.

Cara kerja pelestarian IP klien

Network Load Balancers tidak menyimpan alamat IP klien kecuali Anda menyetel `preserve_client_ip.enabled` atributnya. `true` Selain itu, dengan Dualstack Network Load Balancers, kami mempertahankan alamat IP klien saat menerjemahkan alamat IPv4 ke IPv6. Namun, ketika menerjemahkan alamat IPv6 ke IPv4, IP sumber selalu merupakan alamat IP pribadi dari Network Load Balancer.

Untuk menemukan alamat IP pribadi penyeimbang beban menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Di bidang pencarian, masukkan nama Penyeimbang Beban Jaringan Anda. Ada satu antarmuka jaringan per subnet penyeimbang beban.
4. Pada tab Detail untuk setiap antarmuka jaringan, salin alamat dari alamat IPv4 pribadi.

Untuk informasi selengkapnya, lihat Grup keamanan untuk Network Load Balancer.

ACL Jaringan

Ketika Anda mendaftar intans EC2 sebagai target, Anda harus memastikan bahwa ACL jaringan untuk subnet untuk instans Anda memungkinkan lalu lintas pada port pendengar maupun port pemeriksaan kondis. Daftar kontrol akses jaringan (ACL) default untuk VPC memungkinkan semua lalu lintas masuk dan keluar. Jika Anda membuat ACL jaringan kustom, verifikasi bahwa mereka mengizinkan lalu lintas yang sesuai.

ACL jaringan yang terkait dengan subnet untuk instans Anda harus mengizinkan lalu lintas berikut untuk penyeimbang beban menghadap internet.

Aturan yang disarankan untuk subnet instans

Inbound

Sumber	Protokol	Rentang Port	Komentar
Alamat IP klien	*pendengar*	*pendengar*	Izinkan lalu lintas klien (tipe `instance` target)
VPC CIDR	*pendengar*	*pendengar*	Izinkan lalu lintas klien (tipe `ip` target)
VPC CIDR	*pemeriksaan kesehatan*	*pemeriksaan kesehatan*	Izinkan lalu lintas pemeriksaan kesehatan dari penyeimbang beban

Outbound

Destinasi	Protokol	Rentang Port	Komentar
Alamat IP klien	*pendengar*	*pendengar*	Izinkan tanggapan ke klien (tipe `instance` target)
VPC CIDR	*pendengar*	*pendengar*	Izinkan tanggapan ke klien (tipe `ip` target)
VPC CIDR	*pemeriksaan kesehatan*	1024-65535	Izinkan lalu lintas pemeriksaan kesehatan

Jaringan ACL yang terkait dengan subnet untuk penyeimbang beban Anda harus mengizinkan lalu lintas berikut untuk penyeimbang beban menghadap internet.

Aturan yang disarankan untuk subnet penyeimbang beban

Inbound

Sumber	Protokol	Rentang Port	Komentar
Alamat IP klien	*pendengar*	*pendengar*	Izinkan lalu lintas klien (tipe `instance` target)
VPC CIDR	*pendengar*	*pendengar*	Izinkan lalu lintas klien (tipe `ip` target)
VPC CIDR	*pemeriksaan kesehatan*	1024-65535	Izinkan lalu lintas pemeriksaan kesehatan

Outbound

Destinasi	Protokol	Rentang Port	Komentar

Alamat IP klien	*pendengar*	*pendengar*	Izinkan tanggapan ke klien (tipe `instance` target)
VPC CIDR	*pendengar*	*pendengar*	Izinkan tanggapan ke klien (tipe `ip` target)
VPC CIDR	*pemeriksaan kesehatan*	*pemeriksaan kesehatan*	Izinkan lalu lintas pemeriksaan kesehatan
VPC CIDR	*pemeriksaan kesehatan*	1024-65535	Izinkan lalu lintas pemeriksaan kesehatan

Untuk penyeimbang beban internal, jaringan ACL untuk subnet untuk instans Anda dan simpul penyeimbang beban harus memungkinkan lalu lintas masuk dan keluar ke dan dari VPC CIDR, pada port pendengar dan port fana.

Subnet bersama

Peserta dapat membuat Network Load Balancer di VPC bersama. Peserta tidak dapat mendaftarkan target yang berjalan di subnet yang tidak dibagikan dengan mereka.

Subnet bersama untuk Network Load Balancers didukung di semua AWS Wilayah, tidak termasuk:

- Asia Pasifik (Osaka) `ap-northeast-3`
- Asia Pasifik (Hongkong) `ap-east-1`
- Timur Tengah (Bahrain) `me-south-1`
- AWS Tiongkok (Beijing) `cn-north-1`
- AWS Tiongkok (Ningxia) `cn-northwest-1`

Mendaftarkan atau membatalkan pendaftaran target

Setiap grup target harus memiliki setidaknya satu target yang terdaftar di setiap Availability Zone yang diaktifkan untuk penyeimbang beban.

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

Persyaratan dan pertimbangan

- Anda tidak dapat mendaftarkan instance berdasarkan ID instans jika menggunakan salah satu jenis instance berikut: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M1, M2, M3, atau T1.
- Saat mendaftarkan target dengan ID instance untuk grup target IPv6, target harus memiliki alamat IPv6 primer yang ditetapkan. Untuk mempelajari selengkapnya, lihat alamat IPv6 di Panduan Pengguna Amazon EC2
- Saat mendaftarkan target berdasarkan ID instans, instance harus berada dalam VPC Amazon yang sama dengan Network Load Balancer. Anda tidak dapat mendaftarkan instance berdasarkan ID instans jika berada di VPC yang diintip ke VPC penyeimbang beban (Wilayah yang sama atau Wilayah yang berbeda). Anda dapat mendaftarkan instnas ini dengan alamat IP.
- Jika Anda mendaftarkan target dengan alamat IP dan alamat IP berada di VPC yang sama dengan penyeimbang beban, penyeimbang beban memverifikasi bahwa itu adalah dari subnet yang dapat dicapai.
- Untuk kelompok target UDP dan TCP_UDP, jangan daftarkan instans dengan alamat IP jika mereka berada di luar VPC penyeimbang beban atau jika mereka menggunakan salah satu jenis contoh berikut: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3, atau T1. Target yang berada di luar VPC penyeimbang beban atau menggunakan jenis instans yang tidak didukung mungkin dapat menerima lalu lintas dari penyeimbang beban tetapi kemudian tidak dapat merespons.

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 instans, masukkan port default sesuai kebutuhan, lalu pilihSertakan sebagai tertunda di bawah ini. Setelah selesai menambah instans, pilihMendaftarkan target tertunda.

   Catatan:

   - Instance harus memiliki alamat IPv6 primer yang ditetapkan untuk didaftarkan dengan grup target IPv6.
   - AWS GovCloud (US) Region s tidak mendukung penetapan alamat IPv6 utama menggunakan konsol. Anda harus menggunakan API untuk menetapkan alamat IPv6 utama di s. AWS GovCloud (US) Region
6. Untuk membatalkan pendaftaran instans, pilih instans, lalu pilih Deregister.

Mendaftar atau membatalkan pendaftaran target berdasarkan alamat IP

Target IPv4

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)

Jenis alamat IP tidak dapat diubah setelah grup target dibuat.

Saat meluncurkan Network Load Balancer di VPC Amazon bersama sebagai peserta, Anda hanya dapat mendaftarkan target di subnet yang telah dibagikan dengan Anda.

Target IPv6

- Alamat IP yang Anda daftarkan harus berada di dalam blok VPC CIDR atau dalam blok CIDR VPC yang dipeer.
- Jenis alamat IP tidak dapat diubah setelah grup target dibuat.
- Anda dapat mengaitkan grup target IPv6 hanya ke penyeimbang beban dualstack dengan TCP atau pendengar TLS.

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 menampilkan detailnya.
4. Pilih tabTarget.
5. Untuk mendaftarkan alamat IP, pilihTarget daftar. Untuk setiap alamat IP, pilih jaringan, Availability Zone, alamat IP (IPv4 atau IPv6), dan port, lalu pilih Sertakan sebagai tertunda di bawah ini. Setelah selesai menentukan alamat, pilihMendaftarkan 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

Penggunaan perintahRegister-target untuk menambahkan target dan perintah Target deregister untuk menghapus target.

Application Load Balancers sebagai target

Anda dapat membuat grup target dengan Application Load Balancer tunggal sebagai target, dan mengkonfigurasi Network Load Balancer Anda untuk meneruskan lalu lintas ke sana. Dalam skenario ini, Application Load Balancer mengambil alih keputusan load balancing segera setelah lalu lintas mencapainya. Konfigurasi ini menggabungkan fitur dari kedua penyeimbang beban dan menawarkan keuntungan sebagai berikut:

- Anda dapat menggunakan fitur routing berbasis permintaan layer 7 dari Application Load Balancer dalam kombinasi dengan fitur yang didukung Network Load Balancer, seperti layanan endpoint () dan alamat IP statis.AWS PrivateLink
- Anda dapat menggunakan konfigurasi ini untuk aplikasi yang memerlukan titik akhir tunggal untuk multi-protokol, seperti layanan media yang menggunakan HTTP untuk pensinyalan dan RTP untuk streaming konten.

Anda dapat menggunakan fitur ini dengan Application Load Balancer internal atau yang menghadap ke internet sebagai target Network Load Balancer internal atau yang menghadap ke internet.

Pertimbangan

- Untuk mengaitkan Application Load Balancer sebagai target Network Load Balancer, mereka harus berada di VPC Amazon yang sama dalam akun yang sama.
- Anda dapat mengaitkan Application Load Balancer sebagai target beberapa Network Load Balancer. Untuk melakukan ini, daftarkan Application Load Balancer dengan kelompok target terpisah untuk masing-masing Network Load Balancer individu.
- Setiap Application Load Balancer yang Anda daftarkan dengan Network Load Balancer mengurangi jumlah maksimum target per Availability Zone per Network Load Balancer sebesar 50 (jika penyeimbangan beban lintas zona dinonaktifkan) atau 100 (jika penyeimbangan beban lintas zona diaktifkan). Anda dapat menonaktifkan penyeimbangan beban lintas zona di kedua penyeimbang beban untuk meminimalkan latensi dan menghindari biaya transfer data Regional. Untuk informasi selengkapnya, lihat Kuota untuk Penyeimbang Beban Jaringan Anda.
- Ketika jenis grup target adalah`alb`, Anda tidak dapat mengubah atribut grup target. Atribut ini selalu menggunakan nilai defaultnya.
- Setelah Anda mendaftarkan Application Load Balancer sebagai target, Anda tidak dapat menghapus Application Load Balancer sampai Anda membatalkan pendaftarannya dari semua grup target.

Langkah 1: Buat Application Load Balancer

Sebelum Anda mulai, konfigurasikan grup target yang akan digunakan Application Load Balancer ini. Pastikan Anda memiliki virtual private cloud (VPC) dengan target yang akan Anda daftarkan ke grup sasaran. VPC ini harus memiliki setidaknya satu subnet publik di setiap Availability Zone yang digunakan oleh target Anda.

Untuk membuat Application 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 Buat Penyeimbang Beban.
4. Di bawah Application Load Balancer, pilih Buat.
5. Pada halaman Create Application Load Balancer, di bawah konfigurasi Dasar, tentukan nama Load balancer, Skema, dan jenis alamat IP.
6. Untuk Pendengar, Anda dapat membuat pendengar HTTP atau HTTPS di port apa pun. Namun, Anda harus memastikan bahwa nomor port pendengar ini cocok dengan port grup target di mana Application Load Balancer ini akan berada.
7. Di Availability Zones, lakukan hal berikut:

   a. Untuk VPC, pilih virtual private cloud (VPC) dengan instance atau alamat IP yang Anda sertakan sebagai target Application Load Balancer Anda. Anda harus menggunakan VPC yang sama dengan yang akan Anda gunakan untuk Network Load Balancer Anda. Langkah 3: Buat Network Load Balancer, dan konfigurasikan Application Load Balancer sebagai targetnya

   b. Pilih dua atau lebih Availability Zones dan subnet yang sesuai. Pastikan Availability Zone ini cocok dengan yang diaktifkan untuk Network Load Balancer Anda untuk mengoptimalkan ketersediaan, penskalaan, dan kinerja.
8. Anda dapat Menetapkan grup keamanan ke penyeimbang beban Anda dengan membuat grup keamanan baru atau dengan memilih yang sudah ada.

   Grup keamanan yang Anda pilih harus berisi aturan yang memungkinkan lalu lintas ke port pendengar untuk penyeimbang beban ini. Gunakan blok CIDR (rentang alamat IP) komputer klien sebagai sumber lalu lintas dalam aturan masuk untuk grup keamanan. Hal ini memungkinkan klien untuk mengirim lalu lintas melalui Application Load Balancer ini. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan untuk Application Load Balancer sebagai target Network Load Balancer, lihat Grup keamanan untuk Application Load Balancer di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.
9. Untuk Configure Routing, pilih grup target yang Anda konfigurasikan untuk Application Load Balancer ini. Jika Anda tidak memiliki grup target yang tersedia, dan ingin mengonfigurasi yang baru, lihat Membuat grup target di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.
10. Tinjau konfigurasi Anda, dan pilih Buat penyeimbang beban.

Untuk membuat Application Load Balancer menggunakan AWS CLI

Gunakan perintah create-load-balancer.

Langkah 2: Buat grup target dengan Application Load Balancer sebagai target

Membuat grup target memungkinkan Anda mendaftarkan Application Load Balancer baru atau yang sudah ada sebagai target. Anda hanya dapat menambahkan satu Application Load Balancer per grup target. Application Load Balancer yang sama juga dapat digunakan dalam kelompok target yang terpisah, sebagai target hingga dua Network Load Balancer.

Untuk membuat grup target dan mendaftarkan Application Load Balancer sebagai 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. PilihBuat grup target.
4. Pada halaman Tentukan detail grup, di bawah konfigurasi Dasar, pilih Application Load Balancer.
5. Untuk nama grup Target, masukkan nama untuk grup target Application Load Balancer.
6. Untuk Protokol, hanya TCP yang diizinkan. Pilih Port untuk grup target Anda. Port grup target ini harus cocok dengan port listener Application Load Balancer. Atau, Anda dapat menambahkan atau mengedit port listener pada Application Load Balancer agar sesuai dengan port ini.
7. Untuk VPC, pilih virtual private cloud (VPC) dengan Application Load Balancer untuk mendaftar ke grup target.
8. Untuk pemeriksaan Kesehatan, pilih HTTP atau HTTPS sebagai protokol pemeriksaan Kesehatan. Pemeriksaan kesehatan dikirim ke Application Load Balancer dan diteruskan ke targetnya menggunakan port, protokol, dan jalur ping yang ditentukan. Pastikan Application Load Balancer Anda dapat menerima pemeriksaan kesehatan ini dengan meminta pendengar dengan port dan protokol yang sesuai dengan port dan protokol pemeriksaan kesehatan.
9. (Opsional) Tambahkan satu atau lebih tag sesuai kebutuhan.
10. Pilih Selanjutnya.
11. Pada halaman Register target, pilih Application Load Balancer yang ingin Anda daftarkan sebagai target. Application Load Balancer yang Anda pilih dari daftar harus memiliki listener pada port yang sama dengan grup target yang Anda buat. Anda dapat menambahkan atau mengedit pendengar pada penyeimbang beban ini agar sesuai dengan port grup target atau

kembali ke langkah sebelumnya dan mengubah port yang ditentukan untuk grup target. Jika Anda tidak yakin tentang Application Load Balancer mana yang akan ditambahkan sebagai target, atau tidak ingin menambahkannya pada saat ini, Anda dapat memilih untuk menambahkan Application Load Balancer nanti.

12. PilihBuat grup target.

Untuk membuat grup target dan mendaftarkan Application Load Balancer sebagai target, menggunakan AWS CLI

Gunakan perintah create-target-group dan register-target.

Langkah 3: Buat Network Load Balancer, dan konfigurasikan Application Load Balancer sebagai targetnya

Gunakan langkah-langkah berikut untuk membuat Network Load Balancer dan kemudian konfigurasikan Application Load Balancer sebagai targetnya menggunakan konsol.

Untuk membuat Network Load Balancer dan listener 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 Penyeimbang Beban Jaringan, pilih Buat.
5. Konfigurasi dasar

   Pada panel konfigurasi Dasar, konfigurasikan nama Load balancer, Skema, dan jenis alamat IP.
6. Pemetaan jaringan

   a. Untuk VPC, pilih VPC yang sama dengan yang Anda gunakan untuk target Application Load Balancer Anda. Jika Anda memilih Mengakses Internet untuk Skema, hanya VPC dengan internet gateway yang tersedia untuk dipilih.

   b. Untuk Pemetaan, Pilih satu atau beberapa Availability Zone dan subnet yang sesuai. Sebaiknya pilih Availability Zone yang sama dengan target Application Load Balancer untuk mengoptimalkan ketersediaan, penskalaan, dan performa.

      (Opsional) Untuk menggunakan alamat IP statis, pilih Gunakan alamat IP Elastis di pengaturan IPv4 untuk setiap Availability Zone. Dengan alamat IP statis Anda dapat

menambahkan alamat IP tertentu ke daftar izin untuk firewall, atau Anda dapat membuat kode keras alamat IP dengan klien.

7. Pendengar dan perutean

   a. Defaultnya adalah pendengar yang menerima lalu lintas TCP pada port 80. Hanya pendengar TCP yang dapat meneruskan lalu lintas ke grup target Application Load Balancer. Anda harus menyimpan Protokol sebagai TCP, tetapi Anda dapat memodifikasi Port sesuai kebutuhan.

      Dengan konfigurasi ini, Anda dapat menggunakan pendengar HTTPS pada Application Load Balancer untuk menghentikan lalu lintas TLS.

   b. Untuk tindakan Default, pilih grup target Application Load Balancer untuk meneruskan lalu lintas. Jika Anda tidak melihatnya dalam daftar, atau tidak dapat memilih grup target (karena sudah digunakan oleh Network Load Balancer lain), Anda dapat membuat grup target Application Load Balancer seperti yang ditunjukkan pada. Langkah 2: Buat grup target dengan Application Load Balancer sebagai target

8. Tanda

   (Opsional) Tambahkan tag untuk mengkategorikan penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Tag.

9. Ringkasan

   Tinjau konfigurasi Anda, dan pilih Buat penyeimbang beban.

Untuk membuat Network Load Balancer menggunakan AWS CLI

Gunakan perintah create-load-balancer.

Langkah 4: (Opsional) Buat layanan titik akhir VPC

Untuk menggunakan Network Load Balancer yang Anda atur di langkah sebelumnya sebagai titik akhir untuk konektivitas pribadi, Anda dapat mengaktifkan. AWS PrivateLink Ini membuat koneksi pribadi ke penyeimbang beban Anda sebagai layanan endpoint.

Untuk membuat layanan endpoint VPC menggunakan Network Load Balancer

1. Pada panel navigasi, pilih Load Balancers.
2. Pilih nama Network Load Balancer untuk membuka halaman detailnya.

3. Pada tab Integrasi, perluas VPC Endpoint Services ().AWS PrivateLink
4. Pilih Buat layanan endpoint untuk membuka halaman layanan Endpoint. Untuk langkah-langkah yang tersisa, lihat Membuat layanan endpoint di AWS PrivateLink Panduan.

Tag untuk grup target Anda

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 grup target jika tidak direferensikan oleh tindakan lebih 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 .

Memantau Penyeimbang Beban Jaringan Anda

Anda dapat menggunakan fitur berikut untuk memantau penyeimbang beban, menganalisis pola lalu lintas, dan memecahkan masalah dengan penyeimbang beban dan target Anda.

CloudWatch metrik

Anda dapat menggunakan Amazon CloudWatch untuk mengambil statistik tentang titik data untuk penyeimbang beban 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 Network Load Balancer.

Log Aliran VPC

Anda dapat menggunakan Log Aliran VPC untuk menangkap informasi rinci tentang lalu lintas ke dan dari Penyeimbang Beban Jaringan Anda. Untuk informasi selengkapnya, lihat Log aliran VPC di Panduan Pengguna Amazon VPC.

Buat log alur untuk setiap antarmuka jaringan untuk penyeimbang beban Anda. Ada satu antarmuka jaringan per subnet penyeimbang beban. Untuk mengidentifikasi antarmuka jaringan untuk Penyeimbang Beban Jaringan, cari nama penyeimbang beban di bidang deskripsi antarmuka jaringan.

Ada dua entri untuk setiap koneksi melalui Penyeimbang Beban Jaringan Anda, satu untuk koneksi frontend antara klien dan penyeimbang beban dan yang lainnya untuk koneksi backend antara penyeimbang beban dan target. Jika atribut pelestarian IP klien grup target diaktifkan, koneksi akan muncul ke instance sebagai koneksi dari klien. Jika tidak, IP sumber koneksi adalah alamat IP pribadi penyeimbang beban. Jika grup keamanan instans tidak mengizinkan koneksi dari klien tetapi ACL jaringan untuk subnet penyeimbang beban memungkinkan mereka, log untuk antarmuka jaringan untuk penyeimbang beban menunjukkan “TERIMA OK” untuk koneksi frontend dan backend, sedangkan log untuk antarmuka jaringan untuk tampilkan instans “TOLAK OK” untuk sambungan.

Jika Network Load Balancer memiliki grup keamanan terkait, log alur berisi entri untuk lalu lintas yang diizinkan atau ditolak oleh grup keamanan. Untuk Network Load Balancers dengan pendengar TLS, entri flow log Anda hanya mencerminkan entri yang ditolak.

Log akses

Anda dapat menggunakan log akses untuk menangkap informasi rinci tentang permintaan TLS yang dibuat untuk penyeimbang beban Anda. File log disimpan di Amazon S3. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah dengan target Anda. Untuk informasi selengkapnya, lihat Log akses untuk Penyeimbang Beban Jaringan Anda.

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 Log panggilan API untuk Penyeimbang Beban Jaringan Anda menggunakan AWS CloudTrail.

CloudWatch metrik untuk Network Load Balancer

Elastic Load Balancing menerbitkan titik data ke Amazon CloudWatch untuk penyeimbang beban dan target Anda. CloudWatchmemungkinkan 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 penyeimbang beban 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 ketika permintaan mengalir melalui penyeimbang beban. Jika ada permintaan yang mengalir melalui penyeimbang beban, Elastic Load Balancing mengukur dan mengirimkan metriknya dalam interval 60 detik. Jika tidak ada permintaan yang mengalir melalui penyeimbang beban atau tidak ada data untuk metrik, metrik tidak dilaporkan. Untuk Network Load Balancers dengan grup keamanan, lalu lintas yang ditolak oleh grup keamanan tidak ditangkap dalam metrik. CloudWatch

Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

Penyeimbang Beban Jaringan

Namespace `AWS/NetworkELB` mencakup metrik berikut.

Metrik	Deskripsi
`ActiveFlowCount`	Jumlah total arus bersamaan (atau koneksi) dari klien ke target. Metrik ini mencakup koneksi dalam keadaan SYN_SENT dan ESTABLISHED. Sambungan TCP tidak dihentikan pada penyeimba ng beban, sehingga klien membuka koneksi TCP ke target dianggap sebagai aliran tunggal. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Average`, `Maximum`, dan `Minimum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_TCP`	Jumlah total arus TCP bersamaan (atau koneksi) dari klien ke target. Metrik ini mencakup koneksi dalam status SYN_SENT dan DECORD. Sambungan TCP tidak dihentikan pada penyeimbang beban, sehingga klien membuka koneksi TCP ke target dianggap sebagai aliran tunggal. Kriteria pelaporan: Ada nilai bukan nol Statistik: Statistik yang paling berguna adalah `Average`, `Maximum`, dan `Minimum`.

Metrik	Deskripsi
	Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_TLS`	Jumlah total arus TLS bersamaan (atau koneksi) dari klien ke target. Metrik ini mencakup koneksi dalam status SYN_SENT dan DECORD. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Average`, `Maximum`, dan `Minimum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_UDP`	Jumlah total arus UDP 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`

Metrik	Deskripsi
`ClientTLSNegotiationErrorCount`	Jumlah total jabat tangan TLS yang gagal selama negosiasi antara klien dan pendengar TLS. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `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. Kriteria pelaporan: Selalu dilaporkan. Statistik: Semua Dimensi • `LoadBalancer`
`ConsumedLCUs_TCP`	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda untuk TCP. Anda membayar untuk jumlah LCU yang Anda gunakan per jam. Untuk informasi lebih lanjut, lihat Harga Elastic Load Balancing. Kriteria pelaporan: Ada nilai bukan nol. Statistics: Semua Dimensi • `LoadBalancer`

Metrik	Deskripsi
`ConsumedLCUs_TLS`	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda untuk TLS. Anda membayar untuk jumlah LCU yang Anda gunakan per jam. Untuk informasi lebih lanjut, lihat Harga Elastic Load Balancing. Kriteria pelaporan: Ada nilai bukan nol. Statistics: Semua Dimensi • `LoadBalancer`
`ConsumedLCUs_UDP`	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda untuk UDP. Anda membayar untuk jumlah LCU yang Anda gunakan per jam. Untuk informasi lebih lanjut, lihat Harga Elastic Load Balancing. Kriteria pelaporan: Ada nilai bukan nol. Statistics: Semua Dimensi • `LoadBalancer`
`HealthyHostCount`	Jumlah target yang dianggap sehat. Metrik ini tidak termasuk Application Load Balancer yang terdaftar sebagai target. Kriteria pelaporan: Dilaporkan jika pemeriksaan kondisi diaktifkan. Statistik: Statistik yang paling berguna adalah `Maximum` dan `Minimum`. Dimensi • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Metrik	Deskripsi
`NewFlowCount`	Jumlah total arus baru (atau koneksi) didirikan dari klien ke target dalam periode waktu. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`NewFlowCount_TCP`	Jumlah total arus TCP baru (atau koneksi) didirikan dari klien ke target pada periode waktu. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`NewFlowCount_TLS`	Jumlah total arus TLS baru (atau koneksi) didirikan dari klien ke target dalam periode waktu. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`NewFlowCount_UDP`	Jumlah arus UDP baru (atau koneksi) didirikan dari klien ke target dalam periode waktu. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`PeakPacketsPerSecond`	Kecepatan paket tertinggi (paket diproses sesaat), dikira setiap 10 detik saat selama window sampeling. Metrik ini mencakup lalu lintas pemeriksaan kondisi. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Maximum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`PortAllocationErrorCount`	Jumlah total kesalahan alokasi port sementara selama operasi terjemahan IP klien. Nilai bukan nol menunjukkan koneksi klien yang terputus. Catatan: Network Load Balancer mendukung 55.000 koneksi simultan atau sekitar 55.000 koneksi per menit ke setiap target unik (alamat IP dan port) saat melakukan terjemahan alamat klien. Untuk memperbaiki kesalahan alokasi port, tambahkan lebih banyak target ke grup target. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes`	Jumlah byte yang diproses oleh penyeimbang beban, termasuk header TCP/IP. Jumlah ini mencakup lalu lintas ke dan dari target, minus lalu lintas pemeriksaan kondisi. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`ProcessedBytes_TCP`	Jumlah total byte yang diproses oleh pendengar TCP. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes_TLS`	Jumlah total byte yang diproses oleh pendengar TLS. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes_UDP`	Jumlah total byte diproses oleh pendengar UDP. Kriteria pelaporan: Ada nilai bukan nol Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`ProcessedPackets`	Jumlah paket yang diproses oleh penyeimbang beban. Jumlah ini mencakup lalu lintas ke dan dari target, termasuk lalu lintas pemeriksaan kondisi. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`SecurityGroupBlockedFlowCount_Inbound_ICMP`	Jumlah pesan ICMP baru ditolak oleh aturan masuk dari kelompok keamanan penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`SecurityGroupBlockedFlowCount_Inbound_TCP`	Jumlah aliran TCP baru ditolak oleh aturan masuk dari kelompok keamanan penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`SecurityGroupBlockedFlowCount_Inbound_UDP`	Jumlah arus UDP baru ditolak oleh aturan masuk dari kelompok keamanan penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`SecurityGroupBlockedFlowCount_Outbound_ICMP`	Jumlah pesan ICMP baru ditolak oleh aturan keluar dari kelompok keamanan penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`SecurityGroupBlockedFlowCount_Outbound_TCP`	Jumlah aliran TCP baru ditolak oleh aturan keluar dari grup keamanan penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`SecurityGroupBlockedFlowCount_Outbound_UDP`	Jumlah arus UDP baru ditolak oleh aturan keluar dari kelompok keamanan penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`TargetTLSNegotiationErrorCount`	Jumlah total jabat tangan TLS yang gagal selama negosiasi antara pendengar TLS dan target. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer`
`TCP_Client_Reset_Count`	Jumlah total paket (RST) reset yang dikirim dari klien ke target. Reset ini dihasilkan oleh klien dan diteruskan oleh penyeimbang beban. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrik	Deskripsi
`TCP_ELB_Reset_Count`	Jumlah total paket (RST) reset yang dihasilkan oleh penyeimbang beban. Untuk informasi selengkapnya, lihat Pemecahan Masalah. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`TCP_Target_Reset_Count`	Jumlah total paket (RST) reset yang dikirim dari target ke klien. Reset ini dihasilkan oleh target dan diteruskan oleh penyeimbang beban. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`UnHealthyHostCount`	Jumlah target yang dianggap tidak sehat. Metrik ini tidak termasuk Application Load Balancer yang terdaftar sebagai target. Kriteria pelaporan: Dilaporkan jika pemeriksaan kondisi diaktifkan. Statistik: Statistik yang paling berguna adalah `Maximum` dan `Minimum`. Dimensi • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Metrik	Deskripsi
`UnhealthyRoutingFlowCount`	Jumlah aliran (atau koneksi) yang dirutekan menggunakan tindakan failover routing (gagal terbuka). Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensi metrik untuk Penyeimbang Beban Jaringan

Untuk memfilter metrik penyeimbang beban Anda, gunakan dimensi berikut.

Dimensi	Deskripsi
`AvailabilityZone`	Memfilter data metrik berdasarkan Availability Zone.
`LoadBalancer`	Memfilter data metrik berdasarkan penyeimbang beban. Tentukan penyeimbang beban seperti berikut: net/load-balancer-nama/1234567890123456 (bagian akhir dari ARN penyeimbang beban).
`TargetGroup`	Memfilter data metrik berdasarkan grup target. Tentukan grup target sebagai berikut: targetgroup/target-kelompok-nama/1234567890123456 (bagian akhir dari ARN grup target).

Metrik untuk Penyeimbang Beban Jaringan Anda

CloudWatch menyediakan statistik berdasarkan titik data metrik yang diterbitkan oleh Elastic Load Balancing. Statistik adalah agregasi data metrik selama periode waktu tertentu. Bila Anda meminta statistik, aliran data yang dikembalikan akan diidentifikasi dengan nama metrik dan dimensi. Dimensi adalah pasangan nama/nilai yang merupakan bagian dari identitas metrik. Misalnya, Anda dapat

meminta statistik untuk semua instans EC2 yang sehat di belakang penyeimbang beban yang diluncurkan di Availability Zone tertentu.

Statistik `Minimum` dan `Maximum` mencerminkan nilai minimum dan maksimum titik data yang dilaporkan oleh simpul penyeimbang beban oleh individu di setiap jendela pengambilan sampel. Meningkat maksimum `HealthyHostCount` sesuai dengan penurunan minimum `UnHealthyHostCount`. Disarankan untuk memantau maksimum`HealthyHostCount`, memanggil alarm ketika maksimum `HealthyHostCount` jatuh di bawah minimum yang Anda butuhkan, atau sedang`0`. Ini dapat membantu mengidentifikasi kapan target Anda menjadi tidak sehat. Juga disarankan untuk memantau minimum`UnHealthyHostCount`, memanggil alarm ketika minimum `UnHealthyHostCount` naik di atas`0`. Ini memungkinkan Anda untuk menjadi sadar ketika tidak ada lagi target terdaftar.

Statistik `Sum` adalah nilai agregat di semua simpul penyeimbang beban. Karena metrik menyertakan beberapa laporan per periode, `Sum` hanya berlaku untuk metrik yang diagregasikan di semua simpul penyeimbang beban.

Statistik `SampleCount` adalah jumlah sampel yang diukur. Karena metrik dikumpulkan berdasarkan interval dan peristiwa pengambilan sampel, statistik ini biasanya tidak berguna. Misalnya dengan `HealthyHostCount`, `SampleCount` didasarkan pada jumlah sampel yang dilaporkan setiap simpul penyeimbang beban, bukan jumlah host yang sehat.

Lihat CloudWatch metrik untuk penyeimbang beban Anda

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

Atau, Anda dapat melihat metrik untuk penyeimbang beban menggunakan konsol. CloudWatch

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 penyeimbang beban, lakukan hal berikut:

   a. Di panel navigasi, pilih Penyeimbang Beban.
   b. Pilih penyeimbang beban 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.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Metrik.
3. Pilih namespace NetworkELB.
4. (Opsional) Untuk melihat metrik di semua dimensi, ketik 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/NetworkELB
```

Untuk mendapatkan statistik untuk metrik menggunakan AWS CLI

Gunakan perintah get-metric-statistics 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/NetworkELB \
--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 contoh output:

```
{
    "Datapoints": [
        {
            "Timestamp": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Log akses untuk Penyeimbang Beban Jaringan Anda

Elastic Load Balancing menyediakan log akses yang menangkap informasi terperinci tentang koneksi TLS yang dibuat dengan Network Load Balancer Anda. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

> **Important**
>
> Log akses dibuat hanya jika Network Load Balancer memiliki pendengar TLS dan hanya berisi informasi tentang koneksi TLS.

Log akses adalah fitur opsional Elastic Load Balancing yang dinonaktifkan secara default. Setelah Anda mengaktifkan pencatatan akses untuk penyeimbang beban Anda, Elastic Load Balancing menangkap log sebagai file terkompresi dan menyimpannya dalam bucket Amazon S3 yang Anda tentukan. Anda dapat mengaktifkan atau menonaktifkan log kapan saja.

Anda dapat mengaktifkan enkripsi sisi server dengan kunci enkripsi terkelola Amazon S3 (SSE-S3), atau menggunakan Layanan Manajemen Kunci dengan Kunci Terkelola Pelanggan (SSE-KMS CMK) untuk bucket S3 Anda. Setiap file log akses dienkripsi secara otomatis sebelum disimpan dalam bucket S3 Anda dan didekripsi ketika Anda mengaksesnya. Anda tidak perlu melakukan tindakan apapun karena tidak ada perbedaan dalam cara Anda mengakses file log terenkripsi atau tidak

terenkripsi. Setiap file log dienkripsi dengan kunci unik, yang dienkripsi dengan kunci KMS yang diputar secara teratur. Untuk informasi selengkapnya, lihat Menentukan enkripsi Amazon S3 (SSE-S3) dan Menentukan enkripsi sisi server dengan (SSE-KMS) di Panduan Pengguna Amazon AWS KMS S3.

Tidak ada biaya tambahan untuk log akses. Anda dikenakan biaya penyimpanan untuk Amazon S3, tetapi tidak dikenakan biaya untuk bandwidth yang digunakan oleh Elastic Load Balancing untuk mengirim berkas log ke Amazon S3. Untuk informasi selengkapnya tentang biaya penyimpanan, lihat Harga Amazon S3.

Mengakses file log

Elastic Load Balancing menerbitkan berkas log untuk setiap simpul penyeimbang beban setiap 5 menit. Pengiriman log pada akhirnya konsisten. Penyeimbang beban dapat mengirimkan beberapa log untuk periode yang sama. Hal ini biasanya terjadi jika situs memiliki lalu lintas tinggi.

Nama file log akses menggunakan format berikut:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_net.load-balancer-id_end-time_random-string.log.gz
```

bucket

Nama bucket S3 Anda.

prefix

Prefiks (hierarki logis) di bucket. Jika Anda tidak menentukan prefiks, log ditempatkan pada tingkat akar bucket.

aws-akun-id

Akun AWS ID pemilik.

region

Wilayah untuk penyeimbang beban dan bucket S3 Anda.

yyyy/mm/dd

Tanggal pengiriman log.

load-balancer-id

ID sumber daya penyeimbang beban. Jika ID sumber daya berisi garis miring (/) apa pun, mereka akan diganti dengan titik (.).

akhir zaman

Tanggal dan waktu interval logging berakhir. Misalnya, waktu akhir 20181220T2340Z berisi entri untuk permintaan yang dibuat antara 23:35 dan 23:40.

string acak

String acak yang dihasilkan sistem.

Berikut ini adalah contoh nama berkas log:

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-
loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

Anda dapat menyimpan berkas log dalam bucket selama yang diinginkan, tetapi Anda juga dapat menentukan aturan siklus hidup Amazon S3 untuk mengarsipkan atau menghapus berkas log secara otomatis. Untuk informasi selengkapnya, lihat Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Amazon S3.

Entri akses log

Tabel berikut menjelaskan bidang entri log akses, dalam urutan. Semua bidang dibatasi oleh spasi. Ketika bidang baru diperkenalkan, mereka ditambahkan ke akhir entri log. Ketika memproses berkas log, Anda harus mengabaikan bidang apapun pada akhir entri log yang Anda tidak mengharapkan.

Bidang	Deskripsi
jenis	Jenis pendengar. Satu-satunya nilai yang didukung adalah `tls`.
versi	Versi entri log. Versi saat ini adalah 2.0.
time	Waktu yang direkam pada akhir koneksi TLS, dalam format ISO 8601.
elb	ID sumber daya penyeimbang beban.

Bidang	Deskripsi
pendengar	ID sumber daya pendengar TLS untuk koneksi.
klien:port	Alamat IP dan port klien.
tujuan: port	Alamat IP dan port tujuan. Jika klien terhubung langsung ke penyeimba ng beban, tujuannya adalah pendengar. Jika klien menghubungkan menggunakan layanan VPC endpoint, tujuannya adalah VPC endpoint.
connection_time	Total waktu untuk koneksi selesai, dari awal sampai penutupan, dalam milidetik.
tls_handshake_time	Total waktu untuk jabat tangan TLS untuk menyelesaikan setelah sambungan TCP didirikan, termasuk penundaan clinent-side, dalam milidetik. Kali ini termasuk dalam bidang connection_time.
received_bytes	Hitungan byte yang diterima oleh penyeimbang beban dari klien, setelah dekripsi.
sent_bytes	Hitungan byte yang dikirim oleh penyeimbang beban ke klien, sebelum enkripsi.
incoming_tls_alert	Nilai integer peringatan TLS yang diterima oleh penyeimbang beban dari klien, jika ada. Jika tidak, nilai ini diatur ke -.
chosen_cert_arn	Sertifikat ARN yang disajikan kepada klien. Jika tidak ada klien pesan hello yang valid dikirim, nilai ini diatur ke -.
chosen_cert_serial	Dicadangkan untuk penggunaan masa depan. Nilai ini selalu diatur ke -.
tls_cipher	Suite penyandian dinegosiasikan dengan klien, dalam format OpenSSL. Jika negosiasi TLS tidak lengkap, nilai ini diatur ke -.
tls_protocol_version	Protokol TLS dinegosiasikan dengan klien, dalam format string. Nilai yang mungkin adalah`tlsv10`,`tlsv11`,`tlsv12`, dan`tlsv13`. Jika negosiasi TLS tidak lengkap, nilai ini diatur ke -.
tls_named_group	Dicadangkan untuk penggunaan masa depan. Nilai ini selalu diatur ke -.

Bidang	Deskripsi
domain_name	Nilai ekstensi server_name di klien pesan hello. Nilai ini adalah URL-encoded. Jika tidak ada klien pesan hello yang valid dikirim atau ekstensi tidak hadir, nilai ini diatur ke -.
alpn_fe_protocol	Protokol aplikasi dinegosiasikan dengan klien, dalam format string. Nilai yang mungkin untukadalah `h2`, `http/1.1`, dan `http/1.0`. Jika tidak ada kebijakan ALPN dikonfigurasi dalam pendengar TLS, protokol pencocokan tidak ditemukan, atau tidak ada daftar protokol yang valid dikirim, nilai ini diatur ke -.
alpn_be_protocol	Protokol aplikasi dinegosiasikan dengan target, dalam format string. Nilai yang mungkin untukadalah `h2`, `http/1.1`, dan `http/1.0`. Jika tidak ada kebijakan ALPN dikonfigurasi dalam pendengar TLS, protokol pencocokan tidak ditemukan, atau tidak ada daftar protokol yang valid dikirim, nilai ini diatur ke -.
alpn_client_preference_list	Nilai ekstensi dari application_layer_protocol_negotiation dalam klien pesan hello. Nilai ini adalah URL-encoded. Setiap protokol tertutup dalam tanda kutip ganda dan protokol dipisahkan dengan koma. Jika kebijakan ALPN tidak dikonfigurasi dalam pendengar TLS, klien pesan hello tidak valid dikirim, atau ekstensi tidak ada, nilai ini diatur ke -. String dipotong jika lebih panjang dari 256 byte.
tls_connection_creation_time	Waktu yang direkam pada awal koneksi TLS, dalam format ISO 8601.

Contoh Entri log

Berikut ini adalah contoh entri log. Perhatikan bahwa teks muncul pada beberapa baris hanya untuk memudahkan Anda membaca.

Berikut ini adalah contoh bagi pendengar TLS tanpa kebijakan ALPN.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
```

```
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

Berikut ini adalah contoh bagi pendengar TLS dengan kebijakan ALPN.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

Persyaratan bucket

Bila Anda mengaktifkan akses pencatatan log, Anda harus menentukan bucket S3 untuk log akses. Bucket dapat dimiliki oleh akun yang berbeda dari akun yang memiliki penyeimbang beban. Bucket harus memenuhi persyaratan berikut.

Persyaratan

- Bucket harus ditempatkan di Wilayah yang sama dengan penyeimbang beban.
- Awalan yang Anda tentukan tidak boleh disertakan`AWSLogs`. Kami menambahkan bagian dari nama file dimulai dengan `AWSLogs` setelah nama bucket dan awalan yang Anda tentukan.
- Bucket harus memiliki kebijakan bucket yang memberikan izin untuk menulis log akses ke bucket Anda. Kebijakan bucket adalah kumpulan pernyataan JSON yang ditulis dalam bahasa kebijakan akses untuk menentukan izin akses untuk bucket Anda. Berikut ini adalah contoh kebijakan.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
```

```
            "Resource": "arn:aws:s3:::my-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": ["012345678912"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-bucket/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["012345678912"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
                }
            }
        }
    ]
}
```

Dalam kebijakan sebelumnya, untuk`aws:SourceAccount`, tentukan daftar nomor akun yang log dikirimkan ke bucket ini. Untuk`aws:SourceArn`, tentukan daftar ARN dari sumber daya yang menghasilkan log, dalam formulir`arn:aws:logs:source-region:source-account-id:*`.

Enkripsi

Anda dapat mengaktifkan enkripsi sisi server untuk bucket log akses Amazon S3 Anda dengan salah satu cara berikut:

- Tombol yang Dikelola Amazon S3 (SSE-S3)
- AWS KMS kunci yang disimpan di AWS Key Management Service (SSE-KMS) †

† Dengan log akses Network Load Balancer, Anda tidak dapat menggunakan kunci AWS terkelola, Anda harus menggunakan kunci terkelola pelanggan.

Untuk informasi selengkapnya, lihat Menentukan enkripsi Amazon S3 (SSE-S3) dan Menentukan enkripsi sisi server dengan (SSE-KMS) di Panduan Pengguna Amazon AWS KMS S3.

Kebijakan utama harus mengizinkan layanan untuk mengenkripsi dan mendekripsi log. Berikut ini adalah contoh kebijakan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Mengaktifkan pencatatan akses

Saat mengaktifkan pencatatan akses untuk penyeimbang beban, Anda harus menentukan bucket S3 tempat penyeimbang beban akan menyimpan log. Pastikan Anda memiliki bucket ini dan mengonfigurasi kebijakan bucket yang diperlukan untuk bucket ini. Untuk informasi selengkapnya, lihat Persyaratan bucket.

Untuk mengaktifkan Zona Lokal menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban Anda untuk membuka halaman detailnya.

4. Pada tab Atribut, pilih Edit.
5. Pada halaman Edit load balancer attributes, lakukan hal berikut:
   a. Untuk Monitoring, aktifkan Access logs.
   b. Pilih Browse S3 dan pilih bucket untuk digunakan. Atau, masukkan lokasi bucket S3 Anda, termasuk awalan apa pun.
   c. Pilih Simpan perubahan.

Untuk mengaktifkan pencatatan akses menggunakan AWS CLI

Gunakan perintah modifikasi-atribut-penyeimbang–beban.

Menonaktifkan pencatatan akses

Anda dapat menonaktifkan pengelogan akses untuk penyeimbang beban kapan saja. Setelah menonaktifkan pencatatan akses, log akses Anda tetap berada di bucket S3 sampai Anda menghapusnya. Untuk informasi selengkapnya, lihat Bekerja dengan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk menonaktifkan pengelogan akses menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban Anda untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Untuk Monitoring, matikan log Access.
6. Pilih Simpan perubahan.

Untuk menonaktifkan pencatatan akses menggunakan AWS CLI

Gunakan perintah modify-load-balancer-attributes.

Memproses berkas log akses

Berkas log akses terkompresi. Jika Anda membuka file menggunakan konsol Amazon S3, file tersebut tidak terkompresi dan informasinya ditampilkan. Jika mengunduh file-nya, Anda harus membatalkan kompresinya untuk melihat informasi.

Jika ada banyak permintaan di situs web Anda, penyeimbang beban Anda dapat menghasilkan berkas log dengan gigabyte data. Anda mungkin tidak dapat memproses data dalam jumlah besar menggunakan line-by-line pemrosesan. Oleh karena itu, Anda mungkin harus menggunakan alat analisis yang memberikan solusi pemrosesan paralel. Misalnya, Anda dapat menggunakan alat analisis berikut untuk menganalisis dan memproses log akses:

- Amazon Athena adalah layanan query interaktif yang membuatnya mudah untuk menganalisis data di Amazon S3 menggunakan SQL standar. Untuk informasi selengkapnya, lihat Membuat queri log Penyeimbang Beban Jaringan di Panduan Pengguna Amazon Athena.
- Loggly
- Splunk
- Logika Sumo

Log panggilan API untuk Penyeimbang Beban Jaringan Anda menggunakan AWS CloudTrail

Elastic Load Balancing terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS 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 pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi dalam Elastic Load Balancing, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa lain dalam riwayat Layanan AWS Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di Anda Akun AWS, 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 lainnya Layanan AWS 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 Network 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 tersebut dibuat oleh Layanan AWS 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 Anda Akun AWS, 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 Network Load Balancer 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": "2016-04-01T15:31:48Z",
    "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"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
            "ipAddressType": "ipv4",
            "loadBalancerName": "my-load-balancer",
```

```
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "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": "2016-04-01T15:31:48Z",
    "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/net/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"
}
```

Memecahkan masalah Penyeimbang Beban Jaringan Anda

Informasi berikut dapat membantu Anda memecahkan masalah dengan Penyeimbang Beban Jaringan.

Target yang terdaftar tidak dalam pelayanan

Jika target memakan waktu lebih lama dari yang diharapkan untuk masuk ke status `InService`, mungkin target akan gagal dalam pemeriksaan kesehatan. Target Anda tidak akan masuk dalam pelayanan sampai melewati satu pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat Pemeriksaan kondisi untuk grup target Anda.

Verifikasi bahwa instans Anda gagal pemeriksaan kondisi dan kemudian lakukan pemeriksaan berikut ini:

Grup keamanan tidak mengizinkan lalu lintas

Grup keamanan yang terkait dengan instans harus mengizinkan lalu lintas dari penyeimbang beban menggunakan port pemeriksaan kondisi dan protokol pemeriksaan kondisi. Untuk informasi selengkapnya, lihat Menargetkan grup keamanan.

Daftar kontrol akses jaringan (ACL) tidak memungkinkan lalu lintas

ACL jaringan yang terkait dengan subnet untuk instans Anda dan subnet untuk penyeimbang beban Anda harus memungkinkan pemeriksaan lalu lintas dan kesehatan dari penyeimbang beban. Untuk informasi selengkapnya, lihat ACL Jaringan.

Permintaan tidak dirutekan ke target

Periksa hal berikut:

Grup keamanan tidak mengizinkan lalu lintas

Grup keamanan yang terkait dengan instans harus mengizinkan lalu lintas pada port pendengar dari alamat IP klien (jika target ditentukan oleh ID instans) atau simpul penyeimbang beban (jika target ditentukan oleh alamat IP). Untuk informasi selengkapnya, lihat Menargetkan grup keamanan.

Daftar kontrol akses jaringan (ACL) tidak memungkinkan lalu lintas

ACL jaringan yang terkait dengan subnet untuk VPC Anda harus memungkinkan penyeimbang beban dan target untuk berkomunikasi di kedua arah pada port pendengar. Untuk informasi selengkapnya, lihat ACL Jaringan.

Target berada di Availability Zone yang tidak diaktifkan

Jika Anda mendaftar target di Availability Zone tetapi tidak mengaktifkan Availability Zone, target yang terdaftar ini tidak menerima lalu lintas dari penyeimbang beban.

Instans berada di VPC yang di-peering

Jika Anda memiliki instans dalam VPC yang di-peering dengan VPC penyeimbang beban, Anda harus mendaftarkan mereka dengan penyeimbang beban dengan alamat IP, bukan dengan contoh ID.

Target menerima lebih banyak permintaan pemeriksaan kondisi dari yang diharapkan

Pemeriksaan kondisi untuk Penyeimbang Beban Jaringan didistribusikan dan menggunakan mekanisme konsensus untuk menentukan target kesehatan. Oleh karena itu, target menerima lebih dari jumlah pemeriksaan kesehatan yang dikonfigurasikan melalui pengaturan `HealthCheckIntervalSeconds`.

Target menerima permintaan pemeriksaan kondisi lebih sedikit dari yang diharapkan

Periksa apakah `net.ipv4.tcp_tw_recycle` diaktifkan. Pengaturan ini diketahui menyebabkan masalah dengan penyeimbang beban. Pengaturan `net.ipv4.tcp_tw_reuse` dianggap sebagai alternatif yang lebih aman.

Target yang tidak sehat menerima permintaan dari penyeimbang beban

Ini terjadi ketika semua target yang terdaftar tidak sehat. Jika setidaknya ada satu target terdaftar yang sehat, Network Load Balancer Anda hanya meminta target terdaftar yang sehat.

Ketika hanya ada target terdaftar yang tidak sehat, Network Load Balancer merutekan permintaan ke semua target yang terdaftar, yang dikenal sebagai mode fail-open. Network Load Balancer melakukan ini alih-alih menghapus semua alamat IP dari DNS ketika semua target tidak sehat dan Zona Ketersediaan masing-masing tidak memiliki target yang sehat untuk mengirim permintaan.

Target gagal pemeriksaan kondisi HTTP atau HTTPS karena header host tidak cocok

Header host HTTP dalam permintaan pemeriksaan kondisi berisi alamat IP dari simpul penyeimbang beban dan port pendengar, bukan alamat IP target dan port pemeriksaan kesehatan. Jika Anda memetakan permintaan masuk oleh header host, Anda harus memastikan bahwa pemeriksaan kondisi cocok dengan header host HTTP. Pilihan lain adalah untuk menambahkan layanan HTTP terpisah pada port yang berbeda dan mengkonfigurasi grup target untuk menggunakan port tersebut untuk pemeriksaan kondisi. Atau, pertimbangkan untuk menggunakan pemeriksaan kesehatan TCP.

Tidak dapat mengaitkan grup keamanan dengan penyeimbang beban

Jika Network Load Balancer dibuat tanpa grup keamanan, Network Load Balancer tidak dapat mendukung grup keamanan setelah dibuat. Anda hanya dapat mengaitkan grup keamanan ke penyeimbang beban selama pembuatan, atau ke penyeimbang beban yang ada yang awalnya dibuat dengan grup keamanan.

Tidak dapat menghapus semua grup keamanan

Jika Network Load Balancer dibuat dengan grup keamanan, harus ada setidaknya satu grup keamanan yang terkait dengannya setiap saat. Anda tidak dapat menghapus semua grup keamanan dari penyeimbang beban secara bersamaan.

Peningkatan metrik TCP_ELB_Reset_Count

Untuk setiap permintaan TCP bahwa klien membuat melalui Penyeimbang Beban Jaringan, keadaan sambungan dilacak. Jika tidak ada data yang dikirim melalui koneksi oleh klien atau target lebih lama dari batas waktu idle, koneksi ditutup. Jika klien atau target mengirimkan data setelah periode waktu

habis siaga berlalu, menerima paket TCP RST untuk menunjukkan bahwa sambungan tidak berlaku lagi. Selain itu, jika target menjadi tidak sehat, penyeimbang beban mengirimkan TCP RST untuk paket yang diterima pada koneksi klien yang terkait dengan target, kecuali target yang tidak sehat memicu penyeimbang beban gagal terbuka.

Jika Anda melihat lonjakan `TCP_ELB_Reset_Count` metrik tepat sebelum atau tepat ketika `UnhealthyHostCount` metrik meningkat, kemungkinan paket TCP RST dikirim karena target mulai gagal tetapi tidak ditandai tidak sehat. Jika Anda melihat peningkatan terus-menerus `TCP_ELB_Reset_Count` tanpa target ditandai tidak sehat, Anda dapat memeriksa log aliran VPC untuk klien yang mengirim data pada alur kedaluwarsa.

Waktu koneksi habis untuk permintaan dari target ke penyeimbang bebannya

Periksa apakah pelestarian klien IP diaktifkan pada grup target Anda. Loopback NAT, juga dikenal sebagai hairpinning, tidak didukung saat pelestarian IP klien diaktifkan. Jika instans adalah klien penyeimbang beban yang terdaftar, dan memiliki pelestarian klien IP diaktifkan, sambungan berhasil hanya jika permintaan diarahkan ke instans yang berbeda. Jika permintaan dirutekan ke instance yang sama dengan yang dikirim, waktu koneksi habis karena alamat IP sumber dan tujuan sama.

Jika sebuah instans harus mengirim permintaan ke penyeimbang beban yang terdaftar, lakukan salah satu hal berikut:

- Nonaktifkan pelestarian IP klien.
- Pastikan bahwa kontainer yang harus berkomunikasi, berada di instans kontainer yang berbeda.

Kinerja menurun saat memindahkan target ke Penyeimbang Beban Jaringan

Baik Classic Load Balancers dan Application Load Balancers menggunakan koneksi multiplexing, namun Penyeimbang Beban Jaringan tidak. Oleh karena itu, target Anda dapat menerima lebih banyak koneksi TCP di belakang Penyeimbang Beban Jaringan. Pastikan bahwa target Anda siap untuk menangani volume permintaan koneksi yang mungkin mereka terima.

Kesalahan alokasi port yang menghubungkan melalui AWS PrivateLink

Jika Penyeimbang Beban Jaringan dikaitkan dengan layanan VPC endpoint, mendukung 55.000 koneksi simultan atau sekitar 55.000 koneksi per menit untuk setiap target unik (alamat IP dan port). Jika Anda melebihi koneksi ini, ada kemungkinan peningkatan kesalahan alokasi port. Kesalahan alokasi port dapat dilacak menggunakan metrik. `PortAllocationErrorCount` Untuk memperbaiki kesalahan alokasi port, tambahkan lebih banyak target ke grup target. Untuk informasi selengkapnya, lihat CloudWatch metrik untuk Network Load Balancer.

Koneksi intermiten gagal ketika pelestarian IP klien diaktifkan

Saat pelestarian IP klien diaktifkan, Anda mungkin mengalami batasan koneksi TCP/IP yang terkait dengan penggunaan kembali soket yang diamati pada target. Keterbatasan sambungan ini dapat terjadi ketika klien, atau perangkat NAT di depan klien, menggunakan alamat IP sumber yang sama dan port sumber saat menghubungkan ke beberapa simpul penyeimbang beban secara bersamaan. Jika penyeimbang beban merutekan koneksi ini ke target yang sama, koneksi muncul ke target seolah-olah mereka berasal dari soket sumber yang sama, yang menghasilkan kesalahan koneksi. Jika ini terjadi, klien dapat mencoba lagi (jika koneksi gagal) atau menyambung kembali (jika koneksi terputus). Anda dapat mengurangi jenis kesalahan koneksi dengan meningkatkan jumlah sumber port fana atau dengan meningkatkan jumlah target untuk penyeimbang beban. Anda dapat mencegah jenis kesalahan koneksi ini dengan menonaktifkan pelestarian IP klien atau dengan menonaktifkan penyeimbangan beban lintas zona.

Selain itu, ketika pelestarian IP klien diaktifkan, konektivitas mungkin gagal jika klien yang terhubung ke Network Load Balancer juga terhubung ke target di belakang penyeimbang beban. Untuk mengatasi hal ini, Anda dapat menonaktifkan pelestarian IP klien pada grup target yang terpengaruh. Atau, minta klien Anda terhubung hanya ke Penyeimbang Beban Jaringan, atau hanya ke target, tapi tidak keduanya.

Penundaan koneksi TCP

Ketika penyeimbangan beban lintas zona dan pelestarian IP klien diaktifkan, klien yang terhubung ke IP yang berbeda pada penyeimbang beban yang sama dapat diarahkan ke target yang sama. Jika klien menggunakan port sumber yang sama untuk kedua koneksi ini, target akan menerima apa yang tampaknya merupakan koneksi duplikat, yang dapat menyebabkan kesalahan koneksi dan

keterlambatan TCP dalam membangun koneksi baru. Anda dapat mencegah jenis kesalahan koneksi ini dengan menonaktifkan penyeimbangan beban lintas zona. Untuk informasi selengkapnya, lihat Penyeimbangan beban lintas zona.

Potensi kegagalan saat penyeimbang beban sedang ditetapkan

Salah satu alasan Penyeimbang Beban Jaringan bisa gagal ketika sedang ditetapkan adalah jika Anda menggunakan alamat IP yang sudah ditetapkan atau dialokasikan di tempat lain (misalnya, ditetapkan sebagai alamat IP sekunder untuk instans EC2). Alamat IP ini mencegah penyeimbang beban diatur, dan keadaannya adalah `failed`. Anda dapat mengatasi ini dengan membatalkan alokasi alamat IP terkait dan mencoba kembali proses pembuatan.

Resolusi nama DNS berisi lebih sedikit alamat IP daripada Availability Zone yang diaktifkan

Idealnya Network Load Balancer Anda menyediakan satu alamat IP per Availability Zone yang diaktifkan, ketika mereka memiliki setidaknya satu host sehat di Availability Zone. Ketika tidak ada host yang sehat di Availability Zone tertentu, dan penyeimbangan beban lintas zona dinonaktifkan, alamat IP Network Load Balancer masing-masing AZ tersebut akan dihapus dari DNS.

Misalnya, Network Load Balancer Anda memiliki tiga Availability Zone yang diaktifkan, yang semuanya memiliki setidaknya satu instance target terdaftar yang sehat.

- Jika instance target terdaftar di Availability Zone A menjadi tidak sehat, alamat IP yang sesuai dari Availability Zone A untuk Network Load Balancer akan dihapus dari DNS.
- Jika salah satu dari Availability Zone yang diaktifkan tidak memiliki instans target terdaftar yang sehat, dua alamat IP masing-masing Network Load Balancer akan dihapus dari DNS.
- Jika tidak ada instans target terdaftar yang sehat di semua Availability Zone yang diaktifkan, mode fail-open diaktifkan dan DNS akan menyediakan semua alamat IP dari tiga AZ yang diaktifkan dalam hasilnya.

Memecahkan masalah target yang tidak sehat menggunakan peta sumber daya

Jika target Network Load Balancer gagal dalam pemeriksaan kesehatan, Anda dapat menggunakan peta sumber daya untuk menemukan target yang tidak sehat dan mengambil tindakan berdasarkan

kode alasan kegagalan. Untuk informasi selengkapnya, lihat Peta sumber daya Network Load Balancer.

Peta sumber daya menyediakan dua tampilan: Ikhtisar, dan Peta Target Tidak Sehat. Ikhtisar dipilih secara default dan menampilkan semua sumber daya penyeimbang beban Anda. Memilih tampilan Peta Target Tidak Sehat hanya akan menampilkan target yang tidak sehat di setiap grup target yang terkait dengan Network Load Balancer.

> **Note**
>
> Tampilkan detail sumber daya harus diaktifkan untuk melihat ringkasan pemeriksaan kesehatan dan pesan kesalahan untuk semua sumber daya yang berlaku dalam peta sumber daya. Ketika tidak diaktifkan, Anda harus memilih setiap sumber daya untuk melihat detailnya.

Kolom Grup target menampilkan ringkasan target yang sehat dan tidak sehat untuk setiap kelompok sasaran. Ini dapat membantu menentukan apakah semua target gagal dalam pemeriksaan kesehatan, atau hanya target tertentu yang gagal. Jika semua target dalam kelompok sasaran gagal dalam pemeriksaan kesehatan, periksa pengaturan pemeriksaan kesehatan kelompok sasaran. Pilih nama grup target untuk membuka halaman detailnya di tab baru.

Kolom TargetId menampilkan targetID dan status pemeriksaan kesehatan saat ini untuk setiap target. Ketika target tidak sehat, kode alasan kegagalan pemeriksaan kesehatan ditampilkan. Ketika satu target gagal dalam pemeriksaan kesehatan, pastikan target memiliki sumber daya yang cukup. Pilih ID target untuk membuka halaman detailnya di tab baru.

Memilih Ekspor memberi Anda opsi untuk mengekspor tampilan saat ini dari peta sumber daya Network Load Balancer Anda sebagai PDF.

Verifikasi bahwa instans Anda gagal dalam pemeriksaan kesehatan dan kemudian berdasarkan pemeriksaan kode alasan kegagalan untuk masalah berikut:

- Tidak sehat: Waktu permintaan habis
  - Verifikasi grup keamanan dan daftar kontrol akses jaringan (ACL) yang terkait dengan target Anda dan Network Load Balancer tidak memblokir konektivitas.
  - Pastikan target memiliki kapasitas yang cukup untuk menerima koneksi dari Network Load Balancer.

- Respons pemeriksaan kesehatan Network Load Balancer dapat dilihat di setiap log aplikasi target. Untuk informasi lebih lanjut, lihat Health check kode alasan.

- Tidak sehat: FailedHealthChecks
  - Verifikasi target mendengarkan lalu lintas di port pemeriksaan kesehatan.

> **Saat menggunakan pendengar TLS**
>
> Anda memilih kebijakan keamanan yang digunakan untuk koneksi front-end. Kebijakan keamanan yang digunakan untuk koneksi back-end dipilih secara otomatis berdasarkan kebijakan keamanan front-end yang digunakan.
>
> - Jika pendengar TLS Anda menggunakan kebijakan keamanan TLS 1.3 untuk koneksi front-end, kebijakan keamanan akan digunakan untuk koneksi `ELBSecurityPolicy-TLS13-1-0-2021-06` back-end.
> - Jika pendengar TLS Anda tidak menggunakan kebijakan keamanan TLS 1.3 untuk koneksi front-end, kebijakan keamanan akan digunakan untuk koneksi `ELBSecurityPolicy-2016-08` back-end.
>
> Untuk informasi selengkapnya, lihat Kebijakan keamanan.

  - Verifikasi target menyediakan sertifikat server dan kunci dalam format yang benar yang ditentukan oleh kebijakan keamanan.
  - Verifikasi target mendukung satu atau lebih cipher yang cocok, dan protokol yang disediakan oleh Network Load Balancer untuk membuat jabat tangan TLS.

Kuota untuk Penyeimbang Beban Jaringan Anda

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

Untuk melihat kuota untuk penyeimbang beban jaringan, buka Konsol Service Quotas. Di panel navigasi, pilih Layanan AWSdan pilih Elastic Load Balancing. Anda juga dapat menggunakan perintah describe-account-limits(AWS CLI) untuk Elastic Load Balancing.

Untuk meminta peningkatan kuota, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan formulir peningkatan batas Elastic Load Balancing.

Penyeimbang beban

Kuota AndaAkun AWS memiliki kuota berikut yang terkait dengan Penyeimbang Beban jaringan.

Nama	Default	Dapat Disesuaikan
Sertifikat per Penyeimbang Beban Jaringan	25	Ya
Listener per Penyeimbang Beban Jaringan	50	Tidak
ENI Penyeimbang Beban Jaringan per VPC	1.200	Ya
Penyeimbang Beban Jaringan per Wilayah	50	Ya
Grup Target per Tindakan per Penyeimbang Beban Jaringan	1	Tidak
Subnet per Availability Zone per Penyeimbang Beban Jaringan	500 [2]	Ya
Target per Penyeimbang Beban Jaringan	3.000	Ya

[1] Setiap Network Load Balancer menggunakan satu antarmuka per zona. Kuota diatur pada tingkat VPC. Saat berbagi subnet atau VPC, penggunaan dihitung di semua penyewa.

[2] Jika target terdaftar dengan kelompok sasaran N, itu dihitung sebagai target N menuju batas ini. Setiap Application Load Balancer yang merupakan target Network Load Balancer dihitung sebagai 50 target jika load balancing lintas zona dinonaktifkan atau 100 target jika load balancing lintas zona diaktifkan.

[3] Jika load balancing lintas zona diaktifkan, maksimum adalah 500 target per Load Balancer, berapa pun dari jumlah Availability Zone.

Kelompok-kelompok target

Kuota berikut adalah untuk kelompok target.

Nama	Default	Dapat Disesuaikan
Grup Target per Wilayah	3.000	Ya
Target per per per grup per per per per per per grup target per per per per per per per grup target per per per per per per per grup	1.000	Ya
Target per per per per per per per per per per per per per per per per per per per per per per per per per per per per per per	1	Tidak

[1] Kuota ini dibagi oleh Application Load Balancer dan Penyeimbang Beban dan Penyeimbang Beban jaringan.

Riwayat dokumen untuk Penyeimbang Beban

Tabel berikut menjelaskan rilis untuk Penyeimbang Beban Jaringan.

Perubahan	Deskripsi	Tanggal
Sertifikat RSA 3072-bit dan ECDSA 256/384/521-bit	Rilis ini menambahkan dukungan untuk sertifikat RSA 3072-bit, dan sertifikat Elliptic Curve Digital Signature Algorithm (ECDSA) 256, 384 dan 521-bit via (ACM). AWS Certificate Manager	Januari 19, 2024
Pengakhiran FIPS 140-3 TLS	Rilis ini menambahkan kebijakan keamanan yang menggunakan modul kripotogr afi FIPS 140-3 saat mengakhir i koneksi TLS.	20 November 2023
Afinitas DNS zona	Rilis ini menambahkan dukungan untuk klien yang menyelesaikan DNS penyeimbang beban untuk menerima alamat IP di Availability Zone (AZ) yang sama dengan tempat mereka berada.	12 Oktober 2023
Nonaktifkan pemutusan koneksi target yang tidak sehat	Rilis ini menambahkan dukungan untuk mempertah ankan koneksi aktif ke target yang gagal pemeriksaan kesehatan.	12 Oktober 2023
Pengakhiran koneksi UDP default	Rilis ini menambahkan dukungan untuk mengakhir	12 Oktober 2023

	i koneksi UDP di akhir batas waktu deregistrasi secara default.	
Daftarkan target menggunakan IPv6	Rilis ini menambahkan dukungan untuk mendaftarkan instance sebagai target saat ditangani oleh IPv6.	2 Oktober 2023
Grup keamanan untuk Network Load Balancer	Rilis ini menambahkan dukungan untuk mengaitkan grup keamanan dengan Network Load Balancers Anda saat pembuatan.	10 Agustus 2023
Kesehatan kelompok sasaran	Rilis ini menambahkan dukungan untuk mengonfigurasi jumlah minimum atau persentase target yang harus sehat, dan tindakan apa yang dilakukan penyeimbang beban ketika ambang batas tidak terpenuhi.	17 November 2022
Konfigurasi pemeriksaan kesehatan	Rilis ini memberikan perbaikan pada konfigurasi pemeriksaan kesehatan.	17 November 2022
Penyeimbangan beban lintas zona	Rilis ini menambahkan dukungan untuk mengonfigurasi penyeimbangan beban lintas zona di tingkat grup target.	17 November 2022
Kelompok sasaran IPv6	Rilis ini menambahkan dukungan untuk mengkonfigurasi grup target IPv6 untuk Network Load Balancers.	23 November 2021

Penyeimbang beban internal IPv6	Rilis ini menambahkan dukungan untuk mengkonfi gurasi grup target IPv6 untuk Network Load Balancers.	23 November 2021
TLS 1.3	Rilis ini menambahkan kebijakan keamanan yang mendukung TLS versi 1.3.	Oktober 14, 2021
Application Load Balancers sebagai target	Rilis ini menambahkan dukungan untuk mengkonfi gurasi Application Load Balancer sebagai target Network Load Balancer.	27 September 2021
Pelestarian IP klien	Rilis ini menambahkan dukungan untuk mengkonfi gurasi pelestarian IP klien.	4 Februari 2021
Kebijakan keamanan untuk FS yang mendukung TLS versi 1.2	Rilis ini menambahkan kebijakan keamanan untuk Forward Secrecy (FS) yang mendukung TLS versi 1.2.	24 November 2020
Mode tumpukan ganda	Rilis ini menambahkan dukungan untuk mode dual-stack, yang memungkin kan klien untuk terhubung ke penyeimbang beban menggunakan alamat IPv4 dan alamat IPv6.	13 November 2020
Pengakhiran koneksi pada deregistrasi	Rilis ini menambahkan dukungan untuk menutup koneksi ke target yang dideregistrasi setelah akhir batas waktu deregistrasi.	13 November 2020

Kebijakan ALPN	Rilis ini menambahkan dukungan untuk daftar preferensi Application-Layer Protocol Negosiasi (ALPN).	27 Mei 2020
Sesi lengket	Rilis ini menambahkan dukungan untuk sesi lengket berdasarkan alamat IP sumber dan protokol.	28 Februari 2020
Subnet bersama	Rilis ini menambahkan dukungan untuk menentukan subnet yang dibagikan dengan Anda oleh orang lain. Akun AWS	26 November 2019
Alamat IP pribadi	Rilis ini memungkinkan Anda untuk memberikan alamat IP pribadi dari baris alamat IPv4 subnet yang Anda tentukan saat Anda mengaktif kan Availability Zone untuk penyeimbang beban internal.	25 November 2019
Tambahkan subnet	Rilis ini menambahkan dukungan untuk mengaktifkan Availability Zone tambahan setelah Anda membuat penyeimbang beban.	25 November 2019
Kebijakan keamanan untuk FS	Rilis ini menambahkan dukungan untuk tiga kebijakan keamanan kerahasiaan lanjutan yang telah ditentukan sebelumnya.	8 Oktober 2019

Dukungan SNI	Rilis ini menambahkan dukungan untuk Server Name Indication (SNI).	12 September 2019
Protokol UDP	Rilis ini menambahkan dukungan untuk protokol UDP.	24 Juni 2019
Tersedia di wilayah baru	Rilis ini menambahkan dukungan untuk Network Load Balancers di Wilayah Asia Pasifik (Osaka).	12 Juni 2019
Protokol TLS	Rilis ini menambahkan dukungan untuk protokol TLS.	24 Januari 2019
Penyeimbangan beban lintas zona	Rilis ini menambahkan dukungan untuk memungkin kan penyeimbangan beban lintas zona.	22 Februari 2018
Protokol proxy	Rilis ini menambahkan dukungan untuk mengaktifkan Protokol Proxy.	17 November 2017
Alamat IP sebagai target	Rilis ini menambahkan dukungan untuk mendaftarkan alamat IP sebagai target.	21 September 2017
Jenis penyeimbang beban baru	Rilis Elastic Load Balancing ini memperkenalkan Penyeimba ng Beban Jaringan.	7 September 2017

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