aws

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, TLS, QUIC, dan TCP_QUIC. 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 tindakan default untuk penyeimbang beban Anda.

Untuk informasi selengkapnya, 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 dari klien, ia memilih target dari grup target dalam tindakan default. Ini mencoba mengirim permintaan ke target yang dipilih menggunakan protokol dan port yang Anda tentukan.

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 Memperbarui Availability Zone untuk Network Load Balancer.

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.

Untuk lalu lintas QUIC, penyeimbang beban memilih target menggunakan ID Server yang ditentukan dalam Connection ID (CID). Untuk upaya koneksi awal yang tidak memiliki ID Server, algoritma hash aliran berdasarkan protokol, alamat IP sumber, port sumber, alamat IP tujuan, dan port tujuan

digunakan. Setelah ID Koneksi ditetapkan lalu lintas untuk CID ini akan diarahkan ke target yang sama selama masa pakai CID.

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 instance IDs, 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 menskalakan setiap layanan secara dinamis berdasarkan permintaan.
- Support untuk protokol QUIC dan TCP_QUIC dengan kontrol kemacetan tingkat lanjut, pembentukan koneksi pulang pergi yang lebih sedikit, TLS bawaan, dan migrasi koneksi lintas jaringan.

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

Memulai

Untuk membuat Network Load Balancer menggunakan Konsol Manajemen AWS,, atau AWS CLI AWS CloudFormation, lihat. Buat Penyeimbang Beban Jaringan

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

Harga

Untuk informasi lebih lanjut, lihat Harga Elastic Load Balancing?

Penyeimbang Beban Jaringan

Network Load Balancer berfungsi sebagai titik kontak tunggal untuk klien. Klien mengirim permintaan ke Network Load Balancer, dan Network Load Balancer mengirimkannya ke target, EC2 seperti instance, di satu atau beberapa Availability Zone.

Untuk mengonfigurasi Network Load Balancer, Anda membuat grup target, lalu mendaftarkan target dengan grup target Anda. Network Load Balancer Anda paling efektif jika Anda memastikan bahwa setiap Availability Zone yang diaktifkan memiliki setidaknya satu target 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 Direct Connect.

Daftar Isi

- Pemesanan kapasitas untuk Network Load Balancer

Keadaan penyeimbang beban

Network Load Balancer dapat berada di salah satu status berikut:

`provisioning`

Network Load Balancer sedang disiapkan.

`active`

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

`failed`

Network Load Balancer tidak dapat diatur.

Jenis alamat IP

Anda dapat mengatur jenis alamat IP yang dapat digunakan klien dengan Network Load Balancer Anda.

Network Load Balancers mendukung jenis alamat IP berikut:

`ipv4`

Klien harus terhubung menggunakan IPv4 alamat (misalnya, 192.0.2.1).

`dualstack`

Klien dapat terhubung ke Network Load Balancer menggunakan kedua IPv4 alamat (misalnya, 192.0.2.1) dan IPv6 alamat (misalnya, 2001:0 db 8:85 a 3:0:0:8 a2e: 0370:7334).

Pertimbangan-pertimbangan

- Network Load Balancer berkomunikasi dengan target berdasarkan jenis alamat IP dari kelompok target.
- Untuk mendukung pelestarian IP sumber untuk IPv6 pendengar UDP, pastikan bahwa awalan Aktifkan untuk IPv6 sumber NAT diaktifkan.

- Saat Anda mengaktifkan mode dualstack untuk Network Load Balancer, Elastic Load Balancing menyediakan catatan DNS AAAA untuk Network Load Balancer. Klien yang berkomunikasi dengan Network Load Balancer menggunakan IPv4 alamat menyelesaikan catatan DNS A. Klien yang berkomunikasi dengan Network Load Balancer menggunakan IPv6 alamat menyelesaikan catatan DNS AAAA.
- Akses ke Network Load Balancer 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 Site-to-Site VPN).

Untuk informasi selengkapnya, lihat Memperbarui jenis alamat IP untuk Network Load Balancer.

Batas waktu idle koneksi

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 tidak lagi dilacak. Jika klien atau target mengirimkan data setelah periode timeout idle berlalu, klien menerima paket TCP RST untuk menunjukkan bahwa koneksi tidak lagi valid.

Nilai batas waktu idle default untuk aliran TCP adalah 350 detik, tetapi dapat diperbarui ke nilai apa pun antara 60-6000 detik. Klien atau target dapat menggunakan paket TCP keepalive untuk memulai kembali batas waktu idle. Paket Keepalive yang dikirim untuk mempertahankan koneksi TLS tidak dapat berisi data atau payload.

Batas waktu idle koneksi untuk pendengar TLS adalah 350 detik dan tidak dapat dimodifikasi. 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.

Meskipun 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. Ini tidak dapat diubah.

EC2 instance harus menanggapi permintaan baru dalam waktu 30 detik untuk membuat jalur kembali.

Untuk informasi selengkapnya, lihat Perbarui batas waktu idle.

Atribut penyeimbang beban

Anda dapat mengonfigurasi Network Load Balancer Anda dengan mengedit atributnya. Untuk informasi selengkapnya, lihat Edit atribut penyeimbang beban.

Berikut ini adalah atribut load balancer untuk Network Load Balancers:

`access_logs.s3.enabled`

Menunjukkan apakah log akses yang disimpan di Amazon S3 diaktifkan. Nilai default-nya `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. Nilai default-nya `false`.

`ipv6.deny_all_igw_traffic`

Memblokir akses internet gateway (IGW) ke Network Load Balancer, mencegah akses yang tidak diinginkan ke Network Load Balancer internal Anda melalui gateway internet. Hal ini diatur `false` untuk Network Load Balancers yang menghadap ke internet dan `true` untuk Network Load Balancer internal. Atribut ini tidak mencegah akses internet non-IGW (misalnya, melalui peering, Transit Gateway AWS Direct Connect, atau). Site-to-Site VPN

`load_balancing.cross_zone.enabled`

Menunjukkan apakah penyeimbangan beban lintas zona diaktifkan. Nilai default-nya `false`.

`dns_record.client_routing_policy`

Menunjukkan bagaimana lalu lintas didistribusikan di antara Zona Ketersediaan Network Load Balancers. 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.

`secondary_ips.auto_assigned.per_subnet`

Jumlah alamat IP sekunder untuk dikonfigurasi. Gunakan untuk mengatasi kesalahan alokasi port jika Anda tidak dapat menambahkan target. Rentang yang valid adalah 0 hingga 7. Default-nya adalah 0. Setelah Anda menetapkan nilai ini, Anda tidak dapat menguranginya.

`zonal_shift.config.enabled`

Menunjukkan apakah pergeseran zona diaktifkan. Nilai default-nya `false`.

Penyeimbangan beban lintas zona

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

Nama DNS

Setiap Network Load Balancer menerima nama Domain Name System (DNS) default dengan sintaks berikut: - .elb. *name id region*.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 khusus dan mengaitkannya dengan nama DNS untuk Network Load Balancer Anda. Ketika klien membuat permintaan menggunakan nama domain kustom ini, server DNS menyelesaikannya ke nama DNS untuk Network Load Balancer 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 Network Load Balancer 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 Network Load Balancer Anda. Untuk informasi selengkapnya, lihat Merutekan lalu lintas ke penyeimbang beban ELB di Panduan Pengembang Amazon Route 53.

Network Load Balancer memiliki satu alamat IP per Availability Zone yang diaktifkan. Ini adalah alamat IP dari node Network Load Balancer. Nama DNS dari Network Load Balancer diselesaikan ke alamat ini. Misalnya, misalkan nama domain khusus untuk Network Load Balancer Anda adalah. `example.networkloadbalancer.com` Gunakan nslookup perintah berikut dig atau untuk menentukan alamat IP node Network Load Balancer.

Linux atau Mac

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

Windows

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

Network Load Balancer memiliki catatan DNS untuk node-nya. Anda dapat menggunakan nama DNS dengan sintaks berikut untuk menentukan alamat IP node Network Load Balancer: *az* *name*- *id* .elb. *region*.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
```

Load balancer kesehatan zona

Network Load Balancers memiliki catatan DNS zonal dan alamat IP di Route 53 untuk setiap zona ketersediaan yang diaktifkan. Ketika Network Load Balancer gagal dalam pemeriksaan kesehatan zona untuk zona ketersediaan tertentu, catatan DNS-nya dihapus dari Route 53. Kesehatan zona penyeimbang beban dipantau menggunakan CloudWatch metrik Amazon`ZonalHealthStatus`, memberi Anda lebih banyak wawasan tentang peristiwa yang menyebabkan kegagalan untuk menerapkan tindakan pencegahan untuk memastikan ketersediaan aplikasi yang optimal. Untuk informasi selengkapnya, lihat Penyeimbang Beban Jaringan.

Network Load Balancer dapat gagal dalam pemeriksaan kesehatan zona karena berbagai alasan, menyebabkan mereka menjadi tidak sehat. Lihat di bawah untuk penyebab umum Network Load Balancer yang tidak sehat yang disebabkan oleh pemeriksaan kesehatan zona yang gagal.

Periksa kemungkinan penyebab berikut:

- Tidak ada target sehat untuk penyeimbang beban
- Jumlah target sehat kurang dari minimum yang dikonfigurasi
- Ada pergeseran zona atau pergeseran otomatis zona yang sedang berlangsung
- Lalu lintas secara otomatis dialihkan ke zona sehat karena masalah yang terdeteksi

Buat Penyeimbang Beban Jaringan

Network Load Balancer mengambil permintaan dari klien dan mendistribusikannya ke seluruh target dalam grup target, seperti instance. EC2 Untuk informasi selengkapnya, lihat the section called “Gambaran umum Penyeimbang Beban Jaringan”.

Tugas

- Prasyarat
- Buat penyeimbang beban
- Uji penyeimbang beban
- Langkah selanjutnya

Prasyarat

- Tentukan Availability Zones dan jenis alamat IP mana yang akan didukung aplikasi Anda. Konfigurasikan VPC penyeimbang beban Anda dengan subnet di masing-masing Availability Zone ini. Jika aplikasi akan mendukung keduanya IPv4 dan IPv6 lalu lintas, pastikan bahwa subnet memiliki keduanya IPv4 dan IPv6 CIDRs. Terapkan setidaknya satu target di setiap Availability Zone.
- Pastikan bahwa grup keamanan untuk instance target mengizinkan lalu lintas pada port listener dari alamat IP klien (jika target ditentukan oleh ID instance) atau node penyeimbang beban (jika target ditentukan oleh alamat IP). Untuk informasi selengkapnya, lihat the section called “Menargetkan grup keamanan”.
- Pastikan bahwa kelompok keamanan untuk contoh target memungkinkan lalu lintas dari penyeimbang beban pada port pemeriksaan kesehatan menggunakan protokol pemeriksaan kesehatan.

- Jika Anda berencana untuk memberikan penyeimbang beban dengan alamat IP statis, pastikan bahwa setiap alamat IP Elastic berasal dari kumpulan IPv4 alamat Amazon dan memiliki grup perbatasan jaringan yang sama dengan penyeimbang beban.
- Jika Anda berencana untuk menggunakan pendengar QUIC atau TCP_QUIC, pastikan Network Load Balancer `ipv4` menggunakan jenis alamat dan tidak memiliki grup keamanan yang terkait dengannya.

Buat penyeimbang beban

Sebagai bagian dari pembuatan Network Load Balancer, Anda akan membuat penyeimbang beban, setidaknya satu pendengar, dan setidaknya satu grup target. Penyeimbang beban Anda siap menangani permintaan klien ketika setidaknya ada satu target terdaftar yang sehat di setiap Availability Zone yang diaktifkan.

Console

Membuat penyembang beban yang baru

1. Buka EC2 konsol Amazon 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 nama Load balancer, masukkan nama untuk Network Load Balancer Anda. Nama harus unik dalam set penyeimbang beban Anda di Wilayah. 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. Network Load Balancer yang menghadap ke internet merutekan permintaan dari klien ke target melalui internet. Network Load Balancer internal merutekan permintaan ke target menggunakan alamat IP pribadi.

    c. Untuk jenis alamat IP Load balancer, pilih IPv4apakah klien Anda menggunakan IPv4 alamat untuk berkomunikasi dengan Network Load Balancer atau Dualstack jika klien Anda menggunakan IPv4 keduanya IPv6 dan alamat untuk berkomunikasi dengan Network Load Balancer.

6. Pemetaan jaringan

   a. Untuk VPC, pilih VPC yang Anda siapkan untuk penyeimbang beban Anda. Dengan penyeimbang beban yang menghadap ke internet, hanya VPCs dengan gateway internet yang tersedia untuk dipilih.

   b. Dengan penyeimbang beban dualstack, Anda tidak dapat menambahkan pendengar UDP kecuali Aktifkan awalan untuk IPv6 sumber NAT aktif (awalan sumber NAT per subnet).

   c. Untuk Availability Zones dan subnet, pilih setidaknya satu Availability Zone, dan pilih satu subnet per zona. Perhatikan bahwa subnet yang dibagikan dengan Anda tersedia untuk dipilih.

      Jika Anda memilih beberapa Availability Zone dan memastikan bahwa Anda telah mendaftarkan target di setiap zona yang dipilih, ini meningkatkan toleransi kesalahan aplikasi Anda.

   d. Dengan penyeimbang beban yang menghadap ke internet, Anda dapat memilih alamat IP Elastis untuk setiap Availability Zone. Ini menyediakan penyeimbang beban Anda dengan alamat IP statis.

      Dengan penyeimbang beban internal, Anda dapat memasukkan IPv4 alamat pribadi dari rentang alamat setiap subnet atau biarkan AWS memilih satu untuk Anda.

      Dengan penyeimbang beban dualstack, Anda dapat memasukkan IPv6 alamat dari rentang alamat setiap subnet atau membiarkan AWS memilih satu untuk Anda.

      Untuk penyeimbang beban dengan sumber NAT diaktifkan, Anda dapat memasukkan IPv6 awalan khusus atau membiarkan AWS memilih satu untuk Anda.

7. Grup keamanan

   Kami memilih grup keamanan default untuk VPC penyeimbang beban. Anda dapat memilih grup keamanan tambahan sesuai kebutuhan. Jika Anda tidak memiliki grup keamanan yang memenuhi kebutuhan Anda, pilih buat grup keamanan baru untuk membuatnya sekarang. Untuk informasi selengkapnya, lihat Membuat grup keamanan di Panduan Pengguna Amazon VPC.

> **Warning**
>
> Jika Anda tidak mengaitkan grup keamanan apa pun dengan Network Load Balancer sekarang, Anda tidak dapat mengaitkannya nanti.

> **Warning**
>
> Untuk menggunakan pendengar QUIC atau TCP_QUIC, Network Load Balancer Anda harus tidak memiliki grup keamanan.

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 Default, pilih grup target untuk meneruskan lalu lintas ke.

      Untuk menambahkan grup target lain pilih Tambahkan grup target dan perbarui bobot sesuai kebutuhan.

      Jika Anda tidak memiliki grup target yang memenuhi kebutuhan Anda, pilih Buat grup target untuk membuatnya sekarang. Untuk informasi selengkapnya, lihat Buat grup target.

   c. (Opsional) Pilih Tambahkan tag pendengar dan masukkan kunci tag dan nilai tag.

   d. (Opsional) Pilih Tambahkan pendengar untuk menambahkan pendengar lain (misalnya, pendengar TLS).

9. Pengaturan pendengar yang aman

   Bagian ini hanya muncul jika Anda menambahkan pendengar TLS.

   a. Untuk kebijakan Keamanan, pilih kebijakan keamanan yang memenuhi persyaratan Anda. Untuk informasi selengkapnya, lihat Kebijakan Keamanan.

   b. Untuk sertifikat SSL/TLS server default, pilih Dari ACM sebagai sumber sertifikat. Pilih sertifikat yang Anda sediakan atau impor menggunakan. AWS Certificate Manager Jika Anda tidak memiliki sertifikat yang tersedia di ACM tetapi memiliki sertifikat untuk digunakan dengan penyeimbang beban Anda, pilih Impor sertifikat dan berikan

informasi yang diperlukan. Jika tidak, pilih Minta sertifikat ACM baru. Untuk informasi selengkapnya, lihat AWS Certificate Manager sertifikat di Panduan AWS Certificate Manager Pengguna.

c. (Opsional) Untuk kebijakan ALPN, pilih kebijakan untuk mengaktifkan ALPN. Untuk informasi selengkapnya, lihat the section called “Kebijakan ALPN”.

10. Tag penyeimbang beban

    (Opsional) Perluas tag penyeimbang beban. Pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag. Untuk informasi selengkapnya, lihat Tag.

11. Ringkasan

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

AWS CLI

Membuat penyembang beban yang baru

Gunakan perintah create-load-balancer.

Contoh berikut membuat penyeimbang beban yang menghadap ke internet dengan dua Availability Zone yang diaktifkan dan grup keamanan.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Untuk membuat Network Load Balancer internal

Sertakan `--scheme` opsi seperti yang ditunjukkan pada contoh berikut.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
```

```
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Untuk membuat Network Load Balancer dualstack

Sertakan `--ip-address-type` opsi seperti yang ditunjukkan pada contoh berikut.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --ip-address-type dualstack \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Untuk menambahkan pendengar

Gunakan perintah create-listener. Sebagai contoh, lihat Buat pendengar.

CloudFormation

Membuat penyembang beban yang baru

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'department'
          Value: '123'
```

Untuk menambahkan pendengar

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::Listener. Sebagai contoh, lihat Buat pendengar.

Uji penyeimbang beban

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

Untuk menguji Network Load Balancer

1. Setelah Network Load Balancer 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 didaftarkan atau belum lulus jumlah minimum pemeriksaan kesehatan untuk dianggap sehat. Setelah status setidaknya satu instans sehat, Anda dapat menguji Network Load Balancer Anda. Untuk informasi selengkapnya, lihat Status kondisi target.
5. Di panel navigasi, pilih Load Balancers.
6. Pilih Network Load Balancer yang baru.
7. Salin nama DNS Network Load Balancer (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 selanjutnya

Setelah membuat penyeimbang beban, Anda mungkin ingin melakukan hal berikut:

- Konfigurasikan atribut penyeimbang beban.
- Konfigurasikan atribut grup target.
- [Pendengar TLS] Tambahkan sertifikat ke daftar sertifikat opsional.
- Konfigurasikan fitur pemantauan.

Memperbarui Availability Zone untuk Network Load Balancer

Anda dapat mengaktifkan atau menonaktifkan Availability Zones untuk Network Load Balancer kapan saja. Saat mengaktifkan Availability Zone, Anda harus menentukan satu subnet dari Availability Zone tersebut. Setelah mengaktifkan Availability Zone, penyeimbang beban mulai merutekan permintaan ke target terdaftar di Availability Zone tersebut. Penyeimbang beban Anda paling efektif jika Anda memastikan bahwa setiap Availability Zone yang diaktifkan memiliki setidaknya satu target terdaftar. Mengaktifkan beberapa Availability Zone membantu meningkatkan toleransi kesalahan aplikasi Anda.

Elastic Load Balancing membuat node Network Load Balancer di Availability Zone yang Anda pilih, dan antarmuka jaringan untuk subnet yang dipilih di Availability Zone tersebut. Setiap node Network Load Balancer di Availability Zone menggunakan antarmuka jaringan untuk mendapatkan IPv4 alamat. Anda dapat melihat antarmuka jaringan ini, tetapi mereka tidak dapat dimodifikasi.

Pertimbangan-pertimbangan

- Untuk Network Load Balancers yang menghadap ke internet, subnet yang Anda tentukan harus memiliki setidaknya 8 alamat IP yang tersedia. Untuk Network Load Balancer internal, ini hanya diperlukan jika Anda mengizinkan AWS memilih IPv4 alamat pribadi dari subnet.
- Anda tidak dapat menentukan subnet di Availability Zone terbatas. Namun, Anda dapat menentukan subnet di Availability Zone yang tidak dibatasi dan menggunakan penyeimbangan beban lintas zona untuk mendistribusikan lalu lintas ke target di Availability Zone yang dibatasi.
- Anda tidak dapat menentukan subnet di Zona Lokal.
- Anda tidak dapat menghapus subnet jika Network Load Balancer memiliki asosiasi titik akhir Amazon VPC yang aktif.
- Saat menambahkan kembali subnet yang sebelumnya dihapus, antarmuka jaringan baru dibuat dengan ID yang berbeda.
- Perubahan subnet dalam Availability Zone yang sama harus merupakan tindakan independen. Anda pertama selesai menghapus subnet yang ada, kemudian Anda dapat menambahkan subnet baru.
- Penghapusan subnet dapat memakan waktu hingga 3 menit untuk menyelesaikannya.

Saat membuat Network Load Balancer yang menghadap ke internet, Anda dapat memilih untuk menentukan alamat IP Elastis untuk setiap Availability Zone. Alamat IP elastis menyediakan Network Load Balancer Anda dengan alamat IP statis. Jika Anda memilih untuk tidak menentukan alamat IP Elastis, AWS akan menetapkan satu alamat IP Elastis untuk setiap Availability Zone.

Saat membuat Network Load Balancer internal, Anda dapat memilih untuk menentukan alamat IP pribadi dari setiap subnet. Alamat IP pribadi menyediakan Network Load Balancer Anda dengan alamat IP statis. Jika Anda memilih untuk tidak menentukan alamat IP pribadi, AWS tetapkan satu untuk Anda.

Sebelum memperbarui Availability Zones untuk Network Load Balancer, sebaiknya Anda mengevaluasi potensi dampak apa pun pada koneksi, arus lalu lintas, atau beban kerja produksi yang ada.

⚠ Memperbarui Availability Zone dapat mengganggu

- Ketika subnet dihapus, Elastic Network Interface (ENI) yang terkait dihapus. Hal ini menyebabkan semua koneksi aktif di Availability Zone dihentikan.
- Setelah subnet dihapus, semua target dalam Availability Zone yang terkait dengannya ditandai sebagai`unused`. Hal ini mengakibatkan target tersebut dihapus dari kumpulan target yang tersedia, dan semua koneksi aktif ke target tersebut dihentikan. Ini termasuk koneksi apa pun yang berasal dari Availability Zone lainnya saat menggunakan penyeimbangan beban lintas zona.
- Network Load Balancers memiliki Time To Live (TTL) 60 detik untuk Nama Domain Berkualitas Penuh (FQDN). Ketika Availability Zone yang berisi target aktif dihapus, koneksi klien yang ada mungkin mengalami batas waktu hingga resolusi DNS terjadi lagi, dan lalu lintas dialihkan ke Availability Zone yang tersisa.

Console

Untuk memodifikasi Availability Zones

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih penyeimbang beban.
4. Pada tab Pemetaan jaringan, pilih Edit subnet.
5. Untuk mengaktifkan Availability Zone, pilih kotak centang dan pilih satu subnet. Jika hanya ada satu subnet yang tersedia, itu dipilih untuk Anda.
6. Untuk mengubah subnet untuk Availability Zone yang diaktifkan, pilih salah satu subnet lain dari daftar.

7. Untuk menonaktifkan Availability Zone, kosongkan kotak centang.
8. Pilih Simpan perubahan.

AWS CLI

Untuk memodifikasi Availability Zones

Gunakan perintah set-subnet.

```
aws elbv2 set-subnets \
    --load-balancer-arn load-balancer-arn \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890
```

CloudFormation

Untuk memodifikasi Availability Zones

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref new-subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Memperbarui jenis alamat IP untuk Network Load Balancer

Anda dapat mengonfigurasi Network Load Balancer Anda sehingga klien dapat berkomunikasi dengan Network Load Balancer hanya menggunakan alamat, atau IPv4 menggunakan IPv4 keduanya IPv6 dan alamat (dualstack). Network 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 Network Load Balancer dan memperbaruinya kapan saja.
- Virtual Private Cloud (VPC) dan subnet yang Anda tentukan untuk Network Load Balancer harus memiliki blok CIDR terkait. IPv6 Untuk informasi selengkapnya, lihat IPv6alamat di Panduan EC2 Pengguna Amazon.
- Tabel rute untuk subnet Network Load Balancer harus merutekan lalu lintas. IPv6
- Jaringan ACLs untuk subnet Network Load Balancer harus memungkinkan lalu lintas. IPv6
- Tidak ada pendengar QUIC atau TCP_QUIC yang melekat pada Network Load Balancer.

Console

Untuk memperbarui jenis alamat IP

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih kotak centang untuk Network Load Balancer.
4. Pilih Actions, Edit IP address type.
5. Untuk jenis alamat IP, pilih IPv4untuk mendukung IPv4 alamat saja atau Dualstack untuk mendukung keduanya IPv4 dan IPv6 alamat.
6. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui jenis alamat IP

Gunakan perintah set-ip-address-type.

```
aws elbv2 set-ip-address-type \
    --load-balancer-arn load-balancer-arn \
    --ip-address-type dualstack
```

CloudFormation

Untuk memperbarui jenis alamat IP

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Mengedit atribut untuk Network Load Balancer

Setelah Anda membuat Network Load Balancer, Anda dapat mengedit atributnya.

Atribut penyeimbang beban

- Perlindungan penghapusan
- Penyeimbangan beban lintas zona
- Afinitas DNS Zona Ketersediaan
- Alamat IP sekunder

Perlindungan penghapusan

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

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

Console

Untuk mengaktifkan atau menonaktifkan perlindungan penghapusan

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

2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama Network Load Balancer untuk membuka halaman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Di bawah Perlindungan, aktifkan atau nonaktifkan perlindungan Penghapusan.
6. Pilih Simpan perubahan.

AWS CLI

Untuk mengaktifkan atau menonaktifkan perlindungan penghapusan

Gunakan modify-load-balancer-attributesperintah dengan `deletion_protection.enabled` atribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=deletion_protection.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan atau menonaktifkan perlindungan penghapusan

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya untuk menyertakan `deletion_protection.enabled` atribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "deletion_protection.enabled"
          Value: "true"
```

Penyeimbangan beban lintas zona

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. Untuk informasi selengkapnya, lihat the section called “Penyeimbangan beban lintas zona”.

Console

Untuk mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona untuk penyeimbang beban

1. Buka EC2 konsol Amazon 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.

AWS CLI

Untuk mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona untuk penyeimbang beban

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

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona untuk penyeimbang beban

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancer sumber daya untuk menyertakan `load_balancing.cross_zone.enabled` atribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Afinitas DNS Zona Ketersediaan

Saat menggunakan kebijakan perutean klien default, permintaan yang dikirim ke nama DNS Network Load Balancers Anda akan menerima alamat IP Network Load Balancer yang sehat. Ini mengarah pada distribusi koneksi klien di seluruh Zona Ketersediaan Network Load Balancer. Dengan kebijakan perutean afinitas Availability Zone, kueri DNS klien mendukung alamat IP Network Load Balancer 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 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

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 Network Load Balancer di Availability Zone mereka sendiri. Kueri dapat diselesaikan ke zona lain jika tidak ada alamat IP Network Load Balancer yang sehat di zona mereka sendiri.
- Afinitas Zona Ketersediaan Sebagian — 85 persen afinitas zona

85 persen kueri DNS klien akan mendukung alamat IP Network Load Balancer 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 alamat IP yang sehat di zona mereka. Ketika tidak ada alamat 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 Network Load Balancer yang sehat di semua Zona Ketersediaan Network Load Balancer.

Afinitas Availability Zone membantu merutekan permintaan dari klien ke Network Load Balancer, sedangkan penyeimbangan beban lintas zona digunakan untuk membantu merutekan permintaan dari Network Load Balancer ke target. Saat menggunakan afinitas Availability Zone, penyeimbangan beban lintas zona harus dimatikan, ini memastikan lalu lintas Network Load Balancer 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 Availability Zone Network Load Balancer 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.
- Saat menggunakan afinitas Availability Zone dengan Network Load Balancers dan Route 53 Resolver, kami menyarankan klien menggunakan titik akhir inbound Route 53 Resolver di Availability Zone mereka sendiri.
- 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.

Memantau

Disarankan untuk melacak distribusi koneksi antara Availability Zones, menggunakan metrik Zonal Network Load Balancer. 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

Console

Untuk mengaktifkan afinitas Availability Zone

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih nama Network Load Balancer 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.

AWS CLI

Untuk mengaktifkan afinitas Availability Zone

Gunakan modify-load-balancer-attributesperintah dengan `dns_record.client_routing_policy` atribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes
 "Key=dns_record.client_routing_policy,Value=partial_availability_zone_affinity"
```

CloudFormation

Untuk mengaktifkan afinitas Availability Zone

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya untuk menyertakan `dns_record.client_routing_policy` atribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
```

```
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "dns_record.client_routing_policy"
          Value: "partial_availability_zone_affinity"
```

Alamat IP sekunder

Jika Anda mengalami kesalahan alokasi port dan Anda tidak dapat menambahkan target ke grup target untuk menyelesaikannya, Anda dapat menambahkan alamat IP sekunder ke antarmuka jaringan penyeimbang beban. Untuk setiap zona di mana penyeimbang beban diaktifkan, kami memilih IPv4 alamat dari subnet penyeimbang beban dan menetapkannya ke antarmuka jaringan yang sesuai. Alamat IP sekunder ini digunakan untuk membangun koneksi dengan target. Mereka juga digunakan untuk lalu lintas pemeriksaan kesehatan. Kami menyarankan Anda menambahkan satu alamat IP sekunder untuk memulai, memantau `PortAllocationErrors` metrik, dan menambahkan alamat IP sekunder lainnya hanya jika kesalahan alokasi port tidak diselesaikan.

> **Warning**
>
> Setelah Anda menambahkan alamat IP sekunder, Anda tidak dapat menghapusnya. Satu-satunya cara untuk melepaskan alamat IP sekunder adalah dengan menghapus penyeimbang beban. Sebelum Anda menambahkan alamat IP sekunder, verifikasi bahwa ada cukup IPv4 alamat yang tersedia di subnet penyeimbang beban.

Console

Untuk menambahkan alamat IP sekunder

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

5. Perluas atribut kasus khusus, buka kunci alamat IP Sekunder yang ditetapkan secara otomatis per atribut subnet, dan pilih jumlah alamat IP sekunder.
6. Pilih Simpan perubahan.

AWS CLI

Untuk menambahkan alamat IP sekunder

Gunakan modify-load-balancer-attributesperintah dengan `secondary_ips.auto_assigned.per_subnet` atribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=secondary_ips.auto_assigned.per_subnet,Value=1"
```

Anda dapat menggunakan describe-network-interfacesperintah untuk mendapatkan IPv4 alamat untuk antarmuka jaringan penyeimbang beban. `--filters`Parameter mencakup hasil ke antarmuka jaringan untuk Network Load Balancers dan `--query` parameter selanjutnya mencakup hasil ke penyeimbang beban dengan nama yang ditentukan dan hanya menampilkan bidang yang ditentukan. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws elbv2 describe-network-interfaces \
    --filters "Name=interface-type,Values=network_load_balancer" \
    --query "NetworkInterfaces[?contains(Description,'my-nlb')].
{ID:NetworkInterfaceId,AZ:AvailabilityZone,Addresses:PrivateIpAddresses[*]}"
```

CloudFormation

Untuk menambahkan alamat IP sekunder

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya untuk menyertakan `secondary_ips.auto_assigned.per_subnet` atribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
```

```
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "secondary_ips.auto_assigned.per_subnet"
          Value: "1"
```

Memperbarui grup keamanan untuk Network Load Balancer

Anda dapat mengaitkan grup keamanan dengan Network Load Balancer untuk mengontrol lalu lintas yang diizinkan untuk mencapai dan meninggalkan Network Load Balancer. 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 Network Load Balancer Anda, semua lalu lintas klien dapat mencapai pendengar Network Load Balancer dan semua lalu lintas dapat meninggalkan Network Load Balancer.

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 Network Load Balancer 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 Network Load Balancer meskipun Anda mengaktifkan pelestarian IP klien untuk Network Load Balancer Anda.

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

Daftar Isi

Pertimbangan-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 Network Load Balancer nanti. Kami menyarankan Anda mengaitkan grup keamanan dengan Network Load Balancer saat Anda membuatnya.
- Setelah membuat Network Load Balancer dengan grup keamanan terkait, Anda dapat mengubah grup keamanan yang terkait dengan Network Load Balancer 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, Network Load Balancer 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 Network Load Balancer internal, Anda dapat menentukan rentang CIDR VPC sebagai sumber untuk mengizinkan hanya lalu lintas dari VPC tertentu. Jika ini adalah Network Load Balancer 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
protocol	*client IP address range*	*listener port*	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 EC2 Pengguna Amazon.

Ke luar

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

Contoh: Terima lalu lintas hanya dari Network Load Balancer

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 Network Load Balancer pada port target dan port pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat the section called “Menargetkan grup keamanan”.

Ke dalam

Protokol	Sumber	Rentang port	Komentar
protocol	sg-111112222233333	*target port*	Memungkinkan lalu lintas masuk dari Network Load Balancer pada port target
protocol	sg-111112222233333	*health check*	Memungkinkan lalu lintas masuk dari Network Load Balancer di port pemeriksaan kesehatan

Ke luar

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

Memperbarui grup keamanan terkait

Jika Anda mengaitkan setidaknya satu grup keamanan dengan Network Load Balancer saat membuatnya, Anda dapat memperbarui grup keamanan untuk Network Load Balancer tersebut kapan saja.

Console

Untuk memperbarui grup keamanan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Network Load Balancer.
4. Pada tab Keamanan, pilih Edit.
5. Untuk mengaitkan grup keamanan dengan Network Load Balancer Anda, pilih grup keamanan tersebut. Untuk menghapus grup keamanan dari Network Load Balancer Anda, kosongkan grup keamanan.
6. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui grup keamanan

Gunakan perintah set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --security-groups sg-1234567890abcdef0 sg-0abcdef0123456789
```

CloudFormation

Untuk memperbarui grup keamanan

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
```

```
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
        - !Ref myNewSecurityGroup
```

Perbarui pengaturan keamanan

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

Console

Untuk memperbarui pengaturan keamanan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Network Load Balancer.
4. Pada tab Keamanan, pilih Edit.
5. Di bawah pengaturan Keamanan, hapus Menegakkan aturan masuk tentang PrivateLink lalu lintas.
6. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui pengaturan keamanan

Gunakan perintah set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
```

```
    --enforce-security-group-inbound-rules-on-private-link-traffic off
```

CloudFormation

Untuk memperbarui pengaturan keamanan

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      EnforceSecurityGroupInboundRulesOnPrivateLinkTraffic: off
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Monitor grup keamanan Network Load Balancer

Gunakan `SecurityGroupBlockedFlowCount_Outbound` CloudWatch metrik `SecurityGroupBlockedFlowCount_Inbound` dan untuk memantau jumlah aliran yang diblokir oleh grup keamanan Network Load Balancer. 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 Network Load Balancer. Untuk informasi selengkapnya, lihat Log aliran VPC di Panduan Pengguna Amazon VPC.

Menandai Network Load Balancer

Tag membantu Anda untuk mengkategorikan Network Load Balancers Anda dengan cara yang berbeda. Misalnya, Anda dapat menandai sumber daya berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap Network Load Balancer. Jika Anda menambahkan tag dengan kunci yang sudah dikaitkan dengan Network Load Balancer, itu akan memperbarui nilai tag tersebut.

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

Pembatasan

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

Console

Untuk memperbarui tag untuk penyeimbang beban

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load Balancers.
3. Pilih kotak centang untuk Network Load Balancer.
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 atau Nilai.
7. Untuk menghapus tanda, pilih Hapus di samping tanda.
8. Pilih Simpan perubahan.

AWS CLI

Untuk menambahkan tag

Gunakan perintah add-tag. Contoh berikut menambahkan dua tag.

```
aws elbv2 add-tags \
    --resource-arns load-balancer-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Untuk menghapus tag

Gunakan perintah remove-tag. Contoh berikut menghapus tag dengan kunci yang ditentukan.

```
aws elbv2 remove-tags \
    --resource-arns load-balancer-arn \
    --tag-keys project department
```

CloudFormation

Untuk menambahkan tag

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::LoadBalancersumber daya untuk menyertakan `Tags` properti.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Menghapus Penyeimbang Beban Jaringan

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

Anda tidak dapat menghapus Network Load Balancer jika perlindungan penghapusan diaktifkan. Untuk informasi selengkapnya, lihat Perlindungan penghapusan.

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

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

Console

Untuk menghapus Network Load Balancer

1. Jika Anda memiliki data DNS untuk domain Anda yang mengarah ke Network Load Balancer Anda, arahkan ke lokasi baru dan tunggu perubahan DNS diterapkan sebelum menghapus Network Load Balancer 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 EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
3. Di panel navigasi, pilih Load Balancers.
4. Pilih kotak centang untuk Network Load Balancer.
5. Pilih Tindakan, Hapus penyeimbang beban.

6. Ketika diminta konfirmasi, masukkan **`confirm`** lalu pilih Hapus.

AWS CLI

Untuk menghapus Network Load Balancer

Gunakan perintah delete-load-balancer.

```
aws elbv2 delete-load-balancer \
    --load-balancer-arn load-balancer-arn
```

Lihat peta sumber daya Network Load Balancer

Peta sumber daya Network Load Balancer menyediakan tampilan interaktif arsitektur Network Load Balancers 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 Network Load Balancers Anda.

Untuk melihat peta sumber daya untuk penyeimbang beban Anda

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih Network Load Balancer.
4. Pilih tab Peta sumber daya.

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 Network Load Balancer 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.
  - Listeners - Pilih protokol listeners: port. Sebagai contoh, `TCP:80`.
  - Grup sasaran - Pilih nama grup target. Sebagai contoh, `my-target-group`.
  - Target - Pilih ID target. Sebagai contoh, `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.

CloudWatch log untuk Network Load Balancer

Amazon CloudWatch Logs mendukung log akses Network Load Balancer sebagai log vended, meningkatkan observabilitas dan menyederhanakan debugging untuk pola lalu lintas jaringan. Anda dapat menganalisis log akses Network Load Balancer secara langsung CloudWatch untuk

mendapatkan wawasan tentang koneksi klien, distribusi lalu lintas, dan status koneksi, membantu Anda mengidentifikasi dan memecahkan masalah jaringan dengan lebih cepat.

Anda dapat mengonfigurasi pengiriman log akses Network Load Balancer ke Amazon Logs, Amazon Data Firehose, dan Amazon CloudWatch Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dengan dukungan untuk format Apache Parquet.

> **Important**
>
> Log akses dibuat hanya jika penyeimbang beban memiliki pendengar TLS, dan log hanya berisi informasi tentang permintaan TLS. Akses log merekam permintaan dengan upaya terbaik. Sebaiknya gunakan log akses untuk memahami sifat permintaan, bukan sebagai penghitungan lengkap semua permintaan.

> **Important**
>
> Log akses “warisan” tradisional tetap tersedia untuk Network Load Balancer. Untuk mengelola konfigurasi log akses lama, kunjungi tab Atribut penyeimbang beban Anda. Untuk informasi selengkapnya tentang log Akses “lama”, lihatLog akses untuk Penyeimbang Beban Jaringan Anda.

Dengan integrasi CloudWatch Log ini, Anda dapat melacak pola akses terperinci menggunakan kueri Wawasan CloudWatch Log, membuat filter metrik untuk pemantauan, dan meninjau pola lalu lintas secara real time menggunakan Live Tail.

Anda dapat mengaktifkan CloudWatch log akses Log untuk Network Load Balancer dari tab Integrasi penyeimbang beban di konsol. Untuk mengaktifkan logging, Anda harus masuk sebagai pengguna yang memiliki izin tertentu. Selain itu, Anda harus memberikan izin AWS untuk mengaktifkan log yang akan dikirim.

Untuk izin yang diperlukan untuk setiap tujuan pencatatan, lihat Mengaktifkan pencatatan dari AWS layanan.

Untuk informasi selengkapnya, lihat Apa itu Amazon CloudWatch Logs? .

Untuk informasi harga, lihat CloudWatch Harga Amazon.

Pergeseran zona untuk Network Load Balancer Anda

Peralihan zona adalah kemampuan dalam Amazon Application Recovery Controller (ARC). Dengan pergeseran zona, Anda dapat mengalihkan sumber daya Network Load Balancer dari Availability Zone yang terganggu dengan satu tindakan. Dengan cara ini, Anda dapat terus beroperasi dari Availability Zone sehat lainnya di file AWS Region.

Saat Anda memulai pergeseran zona, Network Load Balancer menghentikan perutean lalu lintas ke target di Availability Zone yang terpengaruh. Koneksi yang ada ke target di Availability Zone yang terpengaruh tidak dihentikan oleh pergeseran zona. Mungkin perlu beberapa menit agar koneksi ini selesai dengan anggun.

Daftar Isi

Sebelum Anda memulai pergeseran zona

- Pergeseran zona dinonaktifkan secara default dan harus diaktifkan pada setiap Network Load Balancer. Untuk informasi selengkapnya, lihat Aktifkan pergeseran zona untuk Network Load Balancer.
- Anda dapat memulai pergeseran zona untuk Network Load Balancer tertentu hanya untuk satu Availability Zone. Anda tidak dapat memulai pergeseran zona untuk beberapa Availability Zone.
- AWS secara proaktif menghapus alamat IP Network Load Balancer zonal dari DNS ketika beberapa masalah infrastruktur berdampak pada layanan. Selalu periksa kapasitas Availability Zone saat ini sebelum Anda memulai pergeseran zona. Jika Anda menggunakan pergeseran zona pada Network Load Balancer, Availability Zone yang terpengaruh oleh pergeseran zona juga kehilangan kapasitas target.
- Selama pergeseran zona pada Network Load Balancers dengan penyeimbangan beban lintas zona diaktifkan, alamat IP penyeimbang beban zonal dihapus dari DNS. Koneksi yang ada ke target di

Zona Ketersediaan yang terganggu tetap ada hingga ditutup secara organik, sementara koneksi baru tidak lagi diarahkan ke target di Zona Ketersediaan yang terganggu.

Untuk informasi selengkapnya, lihat Praktik terbaik untuk pergeseran zona di ARC di Panduan Pengembang Amazon Application Recovery Controller (ARC).

Pengesampingan administratif pergeseran zona

Target yang termasuk dalam Network Load Balancer akan mencakup status baru`AdministrativeOverride`, yang independen dari negara. `TargetHealth`

Ketika pergeseran zona dimulai untuk Network Load Balancer, semua target dalam zona yang digeser dari dianggap diganti secara administratif. Network Load Balancer berhenti merutekan lalu lintas baru ke target yang diganti secara administratif. Koneksi yang ada tetap utuh sampai ditutup secara organik.

`AdministrativeOverride`Negara-negara yang mungkin adalah:

tidak diketahui

Status tidak dapat disebarkan karena kesalahan internal

no_override

Tidak ada penggantian saat ini aktif pada target

zonal_shift_active

Pergeseran zona aktif di Zona Ketersediaan target

zonal_shift_delegated_to_dns

Status pergeseran zona target ini tidak tersedia `DescribeTargetHealth` tetapi dapat dilihat langsung melalui AWS ARC - Zonal Shift API atau konsol.

Aktifkan pergeseran zona untuk Network Load Balancer

Pergeseran zona dinonaktifkan secara default dan harus diaktifkan pada setiap Network Load Balancer. Ini memastikan bahwa Anda dapat memulai pergeseran zona hanya menggunakan Network Load Balancer tertentu yang Anda inginkan. Untuk informasi selengkapnya, lihat the section called “Peralihan zona”.

Prasyarat

Jika Anda mengaktifkan penyeimbangan beban lintas zona untuk penyeimbang beban, setiap kelompok target yang terpasang pada penyeimbang beban harus memenuhi persyaratan berikut sebelum Anda dapat mengaktifkan pergeseran zona.

- Protokol kelompok sasaran harus `TCP` atau`TLS`.
- Jenis kelompok sasaran tidak bole`halb`.
- Penghentian koneksi untuk target yang tidak sehat harus dinonaktifkan.
- Atribut grup `load_balancing.cross_zone.enabled` target harus `true` atau `use_load_balancer_configuration` (default).

Console

Untuk mengaktifkan pergeseran zona

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Network Load Balancer.
4. Pada tab Atribut, pilih Edit.
5. Di bawah konfigurasi perutean Availability Zone, untuk integrasi pergeseran zona ARC, pilih Aktifkan.
6. Pilih Simpan perubahan.

AWS CLI

Untuk mengaktifkan pergeseran zona

Gunakan modify-load-balancer-attributesperintah dengan `zonal_shift.config.enabled` atribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=zonal_shift.config.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan pergeseran zona

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya untuk menyertakan `zonal_shift.config.enabled` atribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        -Key: "zonal_shift.config.enabled"
         Value: "true"
```

Mulai pergeseran zona untuk Network Load Balancer Anda

Pergeseran zona di ARC memungkinkan Anda memindahkan lalu lintas sementara untuk sumber daya yang didukung dari Availability Zone sehingga aplikasi Anda dapat terus beroperasi secara normal dengan Availability Zone lainnya di suatu AWS Wilayah.

Prasyarat

Sebelum memulai, verifikasi bahwa Anda mengaktifkan pergeseran zona untuk penyeimbang beban.

Console

Prosedur ini menjelaskan cara memulai pergeseran zona menggunakan EC2 konsol Amazon. Untuk langkah-langkah memulai pergeseran zona menggunakan konsol ARC, lihat Memulai pergeseran zona di Panduan Pengembang Amazon Application Recovery Controller (ARC).

Untuk memulai pergeseran zona

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

4. Pada tab Integrasi, perluas Amazon Application Recovery Controller (ARC) dan 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.
8. Pilih kotak centang untuk mengetahui bahwa memulai pergeseran zona mengurangi kapasitas aplikasi Anda dengan mengalihkan lalu lintas dari Availability Zone.
9. Pilih Konfirmasi.

AWS CLI

Untuk memulai pergeseran zona

Gunakan start-zonal-shiftperintah Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift start-zonal-shift \
    --resource-identifier load-balancer-arn \
    --away-from use2-az2 \
    --expires-in 2h \
    --comment "zonal shift due to scheduled maintenance"
```

Memperbarui pergeseran zona untuk Network Load Balancer

Anda dapat memperbarui pergeseran zona untuk menetapkan kedaluwarsa baru, atau mengedit atau mengganti komentar untuk pergeseran zona.

Console

Prosedur ini menjelaskan cara memperbarui pergeseran zona menggunakan EC2 konsol Amazon. Untuk langkah-langkah memperbarui pergeseran zona menggunakan konsol Amazon Application Recovery Controller (ARC), lihat Memperbarui pergeseran zona di Panduan Pengembang Amazon Application Recovery Controller (ARC).

Untuk memperbarui pergeseran zona

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Application Load Balancer dengan pergeseran zona aktif.
4. Pada tab Integrasi, perluas Amazon Application Recovery Controller (ARC) dan pilih Update zonal shift.

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

AWS CLI

Untuk memperbarui pergeseran zona

Gunakan update-zonal-shiftperintah Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift update-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE \
    --expires-in 1h \
    --comment "extending zonal shift for scheduled maintenance"
```

Membatalkan pergeseran zona untuk Network Load Balancer

Anda dapat membatalkan pergeseran zona kapan saja sebelum kedaluwarsa. Anda dapat membatalkan pergeseran zona yang Anda mulai, atau pergeseran zona yang AWS dimulai untuk sumber daya untuk latihan yang dijalankan untuk pergeseran otomatis zona.

Console

Prosedur ini menjelaskan cara membatalkan pergeseran zona menggunakan EC2 konsol Amazon. Untuk langkah-langkah membatalkan pergeseran zona menggunakan konsol Amazon Application Recovery Controller (ARC), lihat Membatalkan pergeseran zona di Panduan Pengembang Amazon Application Recovery Controller (ARC).

Untuk membatalkan pergeseran zona

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah PENYEIMBANGAN BEBAN, pilih Penyeimbang beban.
3. Pilih Network Load Balancer dengan pergeseran zona aktif.
4. Pada tab Integrasi, di bawah Amazon Application Recovery Controller (ARC), pilih Batalkan pergeseran zona.

   Ini membuka konsol ARC untuk melanjutkan proses pembatalan.
5. Pilih Batalkan pergeseran zona.
6. Ketika diminta untuk mengonfirmasi, pilih Konfirmasi.

AWS CLI

Untuk membatalkan pergeseran zona

Gunakan cancel-zonal-shiftperintah Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift cancel-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE
```

Pemesanan kapasitas untuk Network Load Balancer

Pemesanan Load balancer Capacity Unit (LCU) memungkinkan Anda untuk memesan kapasitas minimum statis untuk penyeimbang beban Anda. Network Load Balancers secara otomatis menskalakan untuk mendukung beban kerja yang terdeteksi dan memenuhi kebutuhan kapasitas. Ketika kapasitas minimum dikonfigurasi, penyeimbang beban Anda terus meningkat atau turun berdasarkan lalu lintas yang diterima, tetapi juga mencegah kapasitas menjadi lebih rendah dari kapasitas minimum yang dikonfigurasi.

Pertimbangkan untuk menggunakan reservasi LCU dalam situasi berikut:

- Anda memiliki acara mendatang yang akan memiliki lalu lintas tinggi yang tiba-tiba dan tidak biasa dan ingin memastikan penyeimbang beban Anda dapat mendukung lonjakan lalu lintas yang tiba-tiba selama acara berlangsung.
- Anda memiliki lalu lintas runcing yang tidak terduga karena sifat beban kerja Anda untuk waktu yang singkat.

- Anda menyiapkan penyeimbang beban ke on-board atau memigrasikan layanan Anda pada waktu mulai tertentu dan perlu memulai dengan kapasitas tinggi alih-alih menunggu auto-scaling diterapkan.
- Anda memigrasikan beban kerja antara penyeimbang beban dan ingin mengonfigurasi tujuan agar sesuai dengan skala sumber.

Perkirakan kapasitas yang Anda butuhkan

Saat menentukan jumlah kapasitas yang harus Anda pesan untuk penyeimbang beban, sebaiknya lakukan pengujian beban atau meninjau data beban kerja historis yang mewakili lalu lintas yang akan datang yang Anda harapkan. Menggunakan konsol Elastic Load Balancing, Anda dapat memperkirakan berapa banyak kapasitas yang perlu Anda pesan berdasarkan lalu lintas yang ditinjau.

Atau, Anda dapat merujuk ke CloudWatch metrik ProcessedBytesuntuk menentukan tingkat kapasitas yang tepat. Kapasitas untuk penyeimbang beban Anda dicadangkan LCUs, dengan setiap LCU sama dengan 2.2Mbps. Anda dapat menggunakan metrik Max (ProcessedBytes) untuk melihat lalu lintas throughput maksimum per menit pada penyeimbang beban, lalu mengonversi throughput tersebut menjadi LCUs menggunakan tingkat konversi 2.2Mbps sama dengan 1 LCU.

Jika Anda tidak memiliki data beban kerja historis untuk referensi dan tidak dapat melakukan pengujian beban, Anda dapat memperkirakan kapasitas yang dibutuhkan menggunakan kalkulator reservasi LCU. Kalkulator reservasi LCU menggunakan data berdasarkan AWS pengamatan beban kerja historis dan mungkin tidak mewakili beban kerja spesifik Anda. Untuk informasi selengkapnya, lihat Kalkulator Reservasi Unit Kapasitas Load Balancer.

Wilayah yang Didukung

Fitur ini hanya tersedia di Wilayah berikut:

- Timur AS (N. Virginia)
- AS Timur (Ohio)
- AS Barat (Oregon)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)

- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (Stockholm)

Nilai minimum dan maksimum untuk reservasi LCU

Total permintaan reservasi harus minimal 2.750 LCU per Availability Zone. Nilai maksimum ditentukan oleh kuota untuk akun Anda. Untuk informasi selengkapnya, lihat the section called “Unit Kapasitas Load Balancer”.

Minta reservasi Load balancer Capacity Unit untuk Network Load Balancer Anda

Sebelum Anda menggunakan reservasi LCU, tinjau hal-hal berikut:

- Reservasi LCU tidak didukung pada Network Load Balancers menggunakan pendengar TLS.
- Reservasi LCU hanya mendukung pemesanan kapasitas throughput untuk Network Load Balancer. Saat meminta reservasi LCU, ubah kebutuhan kapasitas Anda dari Mbps menjadi LCUs menggunakan tingkat konversi 1 LCU menjadi 2,2 Mbps.
- Kapasitas dicadangkan di tingkat regional dan didistribusikan secara merata di seluruh zona ketersediaan. Konfirmasikan bahwa Anda memiliki cukup target yang didistribusikan secara merata di setiap zona ketersediaan sebelum mengaktifkan reservasi LCU.
- Permintaan reservasi LCU dipenuhi berdasarkan first come first serve, dan tergantung pada kapasitas yang tersedia untuk suatu zona pada saat itu. Sebagian besar permintaan biasanya dipenuhi dalam waktu satu jam, tetapi dapat memakan waktu hingga beberapa jam.
- Untuk memperbarui reservasi yang ada, permintaan sebelumnya harus disediakan atau gagal. Anda dapat meningkatkan kapasitas cadangan sebanyak yang Anda butuhkan, namun Anda hanya dapat mengurangi kapasitas cadangan dua kali per hari.
- Anda akan terus dikenakan biaya untuk kapasitas yang dipesan atau disediakan sampai mereka dihentikan atau dibatalkan.

Console

Untuk meminta reservasi LCU

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

2. Pada panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban.
4. Pada tab Kapasitas, pilih Edit Reservasi LCU.
5. Pilih Estimasi berbasis referensi historis.
6. Pilih periode referensi untuk melihat tingkat LCU cadangan yang direkomendasikan.
7. Jika Anda tidak memiliki beban kerja referensi historis, Anda dapat memilih Perkiraan manual dan memasukkan jumlah yang akan LCUs dipesan.
8. Pilih Simpan.

AWS CLI

Untuk meminta reservasi LCU

Gunakan perintah modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --minimum-load-balancer-capacity CapacityUnits=3000
```

CloudFormation

Untuk meminta reservasi LCU

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-alb
      Type: application
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      MinimumLoadBalancerCapacity:
        CapacityUnits: 3000
```

Perbarui atau batalkan pemesanan Load Balancer Capacity Unit untuk Network Load Balancer Anda

Jika pola lalu lintas untuk penyeimbang beban Anda berubah, Anda dapat memperbarui atau membatalkan reservasi LCU untuk penyeimbang beban Anda.

Console

Untuk memperbarui atau membatalkan reservasi LCU

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban.
4. Pada tab Kapasitas, lakukan salah satu hal berikut:
   a. Untuk memperbarui reservasi LCU pilih Edit Reservasi LCU.
   b. Untuk membatalkan reservasi LCU, pilih Batalkan Kapasitas.

AWS CLI

Untuk membatalkan reservasi LCU

Gunakan perintah modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --reset-capacity-reservation
```

Memantau reservasi Load balancer Capacity Unit untuk Network Load Balancer Anda

Status reservasi

Berikut ini adalah nilai status yang memungkinkan untuk reservasi LCU:

- `pending`- Menunjukkan reservasi sedang dalam proses penyediaan.
- `provisioned`- Menunjukkan kapasitas cadangan siap dan tersedia untuk digunakan.

- `failed`- Menunjukkan permintaan tidak dapat diselesaikan pada saat itu.
- `rebalancing`- Menunjukkan zona ketersediaan telah ditambahkan atau dihapus dan penyeimbang beban menyeimbangkan kembali kapasitas.

Pemanfaatan LCU

Untuk menentukan penggunaan LCU cadangan, Anda dapat membandingkan `ProcessedBytes` metrik per menit dengan per jam. `Sum(ReservedLCUs)` Untuk mengonversi byte per menit ke LCU per jam, gunakan (byte per menit) *8/60/ (10^6) /2.2.

Console

Untuk melihat status reservasi LCU

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih nama penyeimbang beban.
4. Pada tab Kapasitas, Anda dapat melihat Status Reservasi dan nilai LCU Cadangan.

AWS CLI

Untuk memantau status reservasi LCU

Gunakan perintah describe-capacity-reservation.

```
aws elbv2 describe-capacity-reservation \
    --load-balancer-arn load-balancer-arn
```

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 tentukan untuk pendengar menentukan cara penyeimbang beban merutekan permintaan ke target yang Anda daftarkan, seperti instans EC2.

Daftar Isi

Konfigurasi listener

Listener mendukung protokol dan port berikut ini:

- Protokol: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- 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 listener adalah TLS, Anda harus menerapkan setidaknya satu sertifikat server SSL pada listener. Untuk informasi selengkapnya, lihat Sertifikat server.

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.

Anda dapat menggunakan pendengar QUIC untuk menerima lalu lintas QUIC. Network Load Balancer bertindak sebagai penyeimbang beban pass through sesuai dengan. RFC9000 Manfaatkan pendengar QUIC dan backend berkemampuan QUIC untuk mengaktifkan migrasi koneksi tanpa batas untuk perangkat seluler.

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 mendukung TCP dan QUIC pada port yang sama, buat pendengar TCP_QUIC. Grup target untuk pendengar TCP_QUIC harus menggunakan protokol TCP_QUIC.

Pendengar UDP untuk penyeimbang beban dualstack memerlukan grup target. IPv6

WebSockets hanya didukung pada pendengar TCP, TLS, TCP_UDP, dan TCP_QUIC.

Lalu lintas QUIC tidak mendukung negosiasi versi. QUIC v1 adalah satu-satunya versi QUIC yang didukung.

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.

Tindakan default

Saat membuat pendengar, Anda menentukan tindakan default untuk permintaan perutean. Tindakan default meneruskan permintaan ke grup target yang Anda tentukan.

Mendistribusikan lalu lintas ke beberapa kelompok sasaran

Jika Anda menentukan beberapa grup target untuk tindakan default, permintaan akan didistribusikan ke grup target ini berdasarkan bobot relatifnya. Anda harus menentukan bobot dari 0 hingga 999 untuk setiap kelompok target. Kelompok sasaran dengan berat 0 tidak menerima lalu lintas. Setelah Anda menambahkan grup target atau memperbarui bobot grup target, koneksi baru dirutekan berdasarkan bobot grup target baru. Koneksi yang ada tidak terpengaruh dan berlanjut sampai ditutup seperti biasa.

Sebagai contoh, jika Anda menentukan dua kelompok target, masing-masing dengan berat 10, setiap kelompok target menerima setengah permintaan. Jika Anda menentukan dua kelompok target, satu dengan berat 10 dan yang lainnya dengan berat 20, kelompok target dengan berat 20 menerima permintaan dua kali lebih banyak dari kelompok target dengan berat 10.

Kasus penggunaan umum adalah memigrasikan lalu lintas dari satu grup target ke grup target lainnya. Artinya Anda secara bertahap meningkatkan bobot kelompok target baru sambil menurunkan berat kelompok target asli hingga 0. Jika Anda memperbarui bobot grup target ke 0, setelah periode waktu yang singkat, ia tidak menerima koneksi baru dan koneksi yang ada ditutup.

Sesi lengket dan kelompok sasaran tertimbang

Tindakan meneruskan pada pendengar dapat menentukan apakah akan mengaktifkan kelengketan grup target. Saat diaktifkan, kelengketan grup target menyebabkan koneksi berikutnya dari alamat IP sumber yang sama lebih memilih grup target yang dipilih sebelumnya.

Pertimbangan-pertimbangan

- Untuk pendengar TLS, Anda tidak dapat menambahkan grup target TCP dan grup target TLS ke aturan pendengar. Semua kelompok sasaran harus menggunakan protokol yang sama.
- Untuk pendengar TLS, kelengketan grup target tidak didukung.
- Untuk penyeimbang beban dualstack, Anda tidak dapat menambahkan grup target dan grup IPv4 target ke tindakan IPv6 default yang sama. Semua kelompok target dalam tindakan default harus menggunakan jenis alamat IP yang sama.
- Untuk pendengar, jika tindakan maju berisi beberapa grup target dan salah satu dari mereka memiliki kelekatan yang diaktifkan, maka tindakan maju juga harus mengaktifkan kelengketan grup target.

Atribut pendengar

Berikut ini adalah atribut listener untuk Network Load Balancers:

`tcp.idle_timeout.seconds`

Nilai batas waktu idle tcp, dalam hitungan detik. Kisaran yang valid adalah 60-6000 detik. Defaultnya adalah 350 detik.

Untuk informasi selengkapnya, lihat Perbarui batas waktu idle.

Pendengar yang aman

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 Balancer tidak mendukung otentikasi TLS timbal balik (mTLS). Untuk dukungan mTLS, buat pendengar TCP alih-alih pendengar TLS. Penyeimbang beban melewati permintaan apa adanya, sehingga Anda dapat menerapkan mTL pada target.

Network Load Balancers mendukung dimulainya kembali TLS menggunakan PSK untuk TLS 1.3, dan tiket sesi untuk TLS 1.2 dan yang lebih lama. Dimulainya kembali dengan ID sesi, atau ketika beberapa sertifikat dikonfigurasi di listener menggunakan SNI, tidak didukung. Fitur data 0-RTT dan ekstensi early_data tidak diimplementasikan.

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

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 selengkapnya, lihat Tambahkan pendengar dan Memperbarui kebijakan ALPN.

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 tindakan default. 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 untuk Network Load Balancer.
- Anda tidak dapat menggunakan grup IPv4 target dengan pendengar UDP untuk penyeimbang `dualstack` beban.
- Pendengar QUIC dan TCP_QUIC tidak diizinkan pada penyeimbang beban atau penyeimbang `dualstack` beban dengan grup keamanan terkait.
- Pendengar QUIC dan TCP_QUIC tidak diizinkan pada penyeimbang beban dengan grup keamanan terkait.
- Hanya satu pendengar QUIC atau TCP_QUIC yang diizinkan pada Network Load Balancer pada waktu tertentu.
- Pendengar QUIC dan TCP_QUIC tidak diizinkan pada Network Load Balancer yang memiliki pendengar UDP atau TCP_UDP.

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.

Console

Untuk menambahkan pendengar

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, TLS, QUIC, atau TCP_QUIC. Menjaga port default atau ketik port yang berbeda.
6. Untuk tindakan Default, pilih grup target untuk meneruskan lalu lintas ke.

   Untuk menambahkan grup target lain, pilih Tambahkan grup target dan perbarui bobot sesuai kebutuhan.

   Jika Anda tidak memiliki grup target yang memenuhi kebutuhan Anda, pilih Buat grup target untuk membuatnya sekarang. Untuk informasi selengkapnya, lihat Buat grup target.
7. [TLS pendengar] Untuk Kebijakan keamanan, kami sarankan Anda menyimpan kebijakan keamanan default.
8. [Pendengar TLS] Untuk sertifikat SSL/TLS server default, pilih sertifikat default. Anda dapat memilih sertifikat dari salah satu sumber berikut:

   - Jika Anda membuat atau mengimpor sertifikat menggunakan AWS Certificate Manager, pilih Dari ACM, lalu pilih sertifikat dari Sertifikat (dari ACM).
   - Jika Anda mengimpor sertifikat menggunakan IAM, pilih Dari IAM, lalu pilih sertifikat dari Sertifikat (dari IAM).
   - Jika Anda memiliki sertifikat, pilih Impor sertifikat. Pilih Impor ke ACM atau Impor ke IAM. Untuk kunci pribadi Sertifikat, salin dan tempel isi file kunci pribadi (dikodekan PEM). Untuk badan Sertifikat, salin dan tempel isi file sertifikat kunci publik (dikodekan PEM). Untuk Rantai Sertifikat, salin dan tempel konten file rantai sertifikat (dikodekan PEM), kecuali jika Anda menggunakan sertifikat yang ditandatangani sendiri dan tidak penting bahwa browser secara implisit menerima sertifikat.
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. (Opsional) Untuk menambahkan tag, perluas tag Listener. Pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
11. Pilih Tambahkan.
12. [Pendengar TLS] Untuk menambahkan sertifikat ke daftar sertifikat opsional, lihat. Menambahkan sertifikat ke daftar sertifikat

AWS CLI

Untuk membuat grup target

Jika Anda tidak memiliki grup target yang dapat Anda gunakan untuk tindakan default, gunakan create-target-groupperintah untuk membuatnya sekarang. Sebagai contoh, lihat Buat grup target.

Untuk menambahkan pendengar TCP

Gunakan perintah create-listener, menentukan protokol TCP.

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

Untuk menambahkan pendengar TCP dengan beberapa grup target

Gunakan perintah create-listener, tentukan protokol TCP, grup target, dan bobot.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

Untuk menambahkan pendengar TLS

Gunakan perintah create-listener yang menentukan protokol TLS.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
```

```
    --protocol TLS \
    --port 443 \
    --certificates CertificateArn=certificate-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Untuk menambahkan pendengar UDP

Gunakan perintah create-listener yang menentukan protokol UDP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol UDP \
    --port 53 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Untuk menambahkan pendengar QUIC

Gunakan perintah create-listener yang menentukan protokol QUIC.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol QUIC \
    --port 443 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Untuk menambahkan pendengar TCP

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::Listenermenggunakan protokol TCP.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
```

```
          TargetGroupArn: !Ref myTargetGroup
```

Untuk menambahkan pendengar TCP dengan beberapa grup target

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::Listenermenggunakan protokol TCP.

```
Resources:
    myTCPListener:
        Type: 'AWS::ElasticLoadBalancingV2::Listener'
        Properties:
        LoadBalancerArn: !Ref myLoadBalancer
        Protocol: TCP
        Port: 80
        DefaultActions:
            - Type: forward
            ForwardConfig:
                TargetGroups:
                - TargetGroupArn: !Ref myTargetGroup1,
                    Weight: 10
                - TargetGroupArn: !Ref myTargetGroup2,
                    Weight: 30
            TargetGroupStickinessConfig:
                Enabled: true
```

Untuk menambahkan pendengar TLS

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::Listenermenggunakan protokol TLS.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Untuk menambahkan pendengar UDP

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::Listenermenggunakan protokol UDP.

```
Resources:
  myUDPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: UDP
      Port: 53
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Untuk menambahkan pendengar QUIC

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::Listenermenggunakan protokol QUIC.

```
Resources:
  myQUICListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: QUIC
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Sertifikat server untuk Network Load Balancer

Saat membuat pendengar aman untuk Network Load Balancer, Anda harus menerapkan setidaknya satu sertifikat pada penyeimbang beban. 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.

Algoritma kunci yang didukung

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

Sertifikat default

Saat Anda membuat pendengar TLS, Anda harus menentukan setidaknya satu sertifikat. Sertifikat ini dikenal sebagai Sertifikat default. Anda dapat mengganti sertifikat default setelah Anda membuat TLS pendengar. Untuk informasi selengkapnya, lihat Mengganti 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 kunci publik (lebih suka ECDSA daripada RSA)
- Algoritma 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 untuk Network Load Balancer

Ketika Anda membuat pendengar TLS, Anda harus memilih kebijakan keamanan. Kebijakan keamanan menentukan sandi dan protokol mana yang didukung selama negosiasi SSL antara penyeimbang beban dan klien Anda. Anda dapat memperbarui kebijakan keamanan untuk penyeimbang beban jika persyaratan Anda berubah atau saat kami merilis kebijakan keamanan baru. Untuk informasi selengkapnya, lihat Memperbarui kebijakan keamanan.

Pertimbangan

- Pendengar TLS memerlukan kebijakan keamanan. Jika Anda tidak menentukan kebijakan keamanan saat membuat listener, kami menggunakan kebijakan keamanan default. Kebijakan keamanan default bergantung pada cara Anda membuat listener TLS:
  - Konsol — Kebijakan keamanan default adalah`ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09`.
  - Metode lain (misalnya, AWS CLI, AWS CloudFormation, dan AWS CDK) — Kebijakan keamanan default adalah`ELBSecurityPolicy-2016-08`.
- Kebijakan keamanan dengan PQ dalam nama mereka menawarkan pertukaran kunci pasca-kuantum hibrida. Untuk kompatibilitas, mereka mendukung algoritma pertukaran kunci ML-KEM klasik dan pasca-kuantum. Klien harus mendukung pertukaran kunci ML-KEM untuk menggunakan

TLS pasca-kuantum hibrida untuk pertukaran kunci. Kebijakan pasca-kuantum hibrida mendukung algoritma Secp256R1, Secp384r1 dan MLKEM768 X25519. MLKEM1024 MLKEM768 Untuk informasi lebih lanjut, lihat Post-Quantum Cryptography.

- AWS merekomendasikan penerapan kebijakan keamanan berbasis TLS pasca-kuantum (PQ-TLS) baru atau. `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09` `ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09` Kebijakan ini memastikan kompatibilitas mundur dengan mendukung klien yang mampu menegosiasikan hybrid PQ-TLS, TLS 1.3 saja, atau TLS 1.2 saja, sehingga meminimalkan gangguan layanan selama transisi ke kriptografi pasca-kuantum. Anda dapat bermigrasi secara progresif ke kebijakan keamanan yang lebih ketat saat aplikasi klien Anda mengembangkan kemampuan untuk menegosiasikan PQ-TLS untuk operasi pertukaran kunci.
- 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 log dan Contoh Query Network Load Balancer.
- Untuk melihat versi protokol TLS (posisi bidang log 5) dan pertukaran kunci (posisi bidang log 13) untuk permintaan akses ke penyeimbang beban Anda, aktifkan pencatatan akses dan periksa entri log yang sesuai. Untuk informasi selengkapnya, lihat Log akses.
- Anda dapat membatasi kebijakan keamanan 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 SCPs (), masing-masing. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan (SCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan yang hanya mendukung TLS 1.3 mendukung Forward Secrecy (FS). Kebijakan yang mendukung TLS 1.3 dan TLS 1.2 yang hanya memiliki cipher dari bentuk TLS_* dan ECDHE_* juga menyediakan FS.
- Network Load Balancers mendukung ekstensi Extended Master Secret (EMS) untuk TLS 1.2.

Koneksi Backend

Anda dapat memilih kebijakan keamanan yang digunakan untuk koneksi front-end, tetapi tidak koneksi backend. Kebijakan keamanan untuk koneksi backend bergantung pada kebijakan keamanan pendengar. Jika ada pendengar Anda yang menggunakan:

- Kebijakan TLS pasca-kuantum FIPS - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09`

- Kebijakan FIPS - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`
- Kebijakan TLS pasca-kuantum - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-PQ-2025-09`
- Kebijakan TLS 1.3 - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-2021-06`
- Semua kebijakan TLS lainnya menggunakan koneksi backend `ELBSecurityPolicy-2016-08`

Anda dapat menggambarkan protokol dan cipher menggunakan describe-ssl-policies AWS CLI perintah, atau merujuk ke tabel di bawah ini.

Kebijakan Keamanan

- Kebijakan keamanan TLS
  - Protokol berdasarkan kebijakan
  - Cipher berdasarkan kebijakan
  - Kebijakan oleh cipher
- Kebijakan keamanan FIPS
  - Protokol berdasarkan kebijakan
  - Cipher berdasarkan kebijakan
  - Kebijakan oleh cipher
- FS mendukung kebijakan keamanan
  - Protokol berdasarkan kebijakan
  - Cipher berdasarkan kebijakan
  - Kebijakan oleh cipher

Kebijakan keamanan TLS

Anda dapat menggunakan kebijakan keamanan TLS untuk memenuhi standar kepatuhan dan keamanan yang mengharuskan menonaktifkan versi protokol TLS tertentu, atau untuk mendukung klien lama yang memerlukan cipher usang.

Kebijakan yang hanya mendukung TLS 1.3 mendukung Forward Secrecy (FS). Kebijakan yang mendukung TLS 1.3 dan TLS 1.2 yang hanya memiliki cipher dari bentuk TLS_* dan ECDHE_* juga menyediakan FS.

Daftar Isi

Protokol berdasarkan kebijakan

Tabel berikut menjelaskan protokol yang didukung oleh setiap kebijakan keamanan TLS.

Kebijakan Keamanan	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityKebijakan- TLS13 -1-3-2021-06	Ya	Tidak	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-3-PQ-2025-09	Ya	Tidak	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-2021-06	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06	Ya	Ya	Tidak	Tidak

Kebijakan Keamanan	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-1-2021-06	Ya	Ya	Ya	Tidak
ELBSecurityKebijakan- TLS13 -1-0-2021-06	Ya	Ya	Ya	Ya
ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09	Ya	Ya	Ya	Ya
ELBSecurityKebijakan-TLS-1-2-EXT-2018-06	Tidak	Ya	Tidak	Tidak
ELBSecurityKebijakan-TLS-1-2-2017-01	Tidak	Ya	Tidak	Tidak
ELBSecurityKebijakan-TLS-1-1-2017-01	Tidak	Ya	Ya	Tidak
ELBSecurityKebijakan-2016-08	Tidak	Ya	Ya	Ya
ELBSecurityKebijakan-2015-05	Tidak	Ya	Ya	Ya

Cipher berdasarkan kebijakan

Tabel berikut menjelaskan cipher yang didukung oleh setiap kebijakan keamanan TLS.

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-3-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-3-PQ-2025-09	• TLS_ _ _ CHACHA20 POLY1305 SHA256
ELBSecurityKebijakan- TLS13 -1-2-2021-06 ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ _ _ CHACHA20 POLY1305 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ _ _ CHACHA20 POLY1305 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-2-Ext2 -2021-06 ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ _ _ CHACHA20 POLY1305 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-2-Ext1 -2021-06 ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ _ _ CHACHA20 POLY1305 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-1-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ _ _ CHACHA20 POLY1305 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-0-2021-06 ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ _ _ CHACHA20 POLY1305 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan-TLS-1-2-EXT-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan-TLS-1-2-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Kebijakan keamanan	Cipher
ELBSecurityKebijakan-TLS-1-1-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan-2016-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan-2015-05	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan oleh cipher

Tabel berikut menjelaskan kebijakan keamanan TLS yang mendukung setiap cipher.

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — TLS_AES_128_GCM_ SHA256 IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-3-2021-06 • ELBSecurityKebijakan- TLS13 -1-3-PQ-2025-09	1301

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09	

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-3-2021-06 • ELBSecurityKebijakan- TLS13 -1-3-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09	1302

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL - TLS _ _ _ CHACHA20 POLY1305 SHA256 IANA - TLS_ _ _ CHACHA20 POLY1305 SHA256	• ELBSecurityKebijakan- TLS13 -1-3-2021-06 • ELBSecurityKebijakan- TLS13 -1-3-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09	1303

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL - 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c02b

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_DENGAN_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c02f

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL - 128-SHA256 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c023

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 128-SHA256 IANA — TLS_ECDHE_RSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c027

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-ECDSA-AES 128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c009

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-RSA-AES 128-SHA IANA — TLS_ECDHE_RSA_WITH _AES_128_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c013

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL - 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c02c

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 256-GCM- SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Re-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-RES-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c030

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_256_CBC_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c024

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_RSA_DENGAN_AES_256_CBC_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c028

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-ECDSA-AES 256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c00a

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-RSA-AES 256-SHA IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	c014

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
AES128OpenSSL — -GCM- SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	9c

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
AES128OpenSSL — - SHA256 IANA — TLS_RSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	3c

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — AES128 -SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	2f

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
AES256OpenSSL — -GCM- SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	9d

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
AES256OpenSSL — - SHA256 IANA — TLS_RSA_DENGAN_AES_256_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-Ext1-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-2-2017-01 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	3d

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — AES256 -SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-Ext2-2021-06 • ELBSecurityKebijakan- TLS13 -1-2-Ext2-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-2021-06 • ELBSecurityKebijakan- TLS13 -1-0-PQ-2025-09 • ELBSecurityKebijakan-TLS-1-2-EXT-2018-06 • ELBSecurityKebijakan-TLS-1-1-2017-01 • ELBSecurityKebijakan-2016-08	35

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.

> **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 FIPS140 modul, mereka mungkin tidak sesuai dengan panduan NIST terbaru untuk konfigurasi TLS.

Daftar Isi

Protokol berdasarkan kebijakan

Tabel berikut menjelaskan protokol yang didukung oleh setiap kebijakan keamanan FIPS.

Kebijakan Keamanan	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityKebijakan- TLS13 -1-3-FIPS-2023-04	Ya	Tidak	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-3-FIPS-PQ-2025-09	Ya	Tidak	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04	Ya	Ya	Tidak	Tidak

Kebijakan Keamanan	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09	Ya	Ya	Tidak	Tidak
ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04	Ya	Ya	Ya	Tidak
ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04	Ya	Ya	Ya	Ya
ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	Ya	Ya	Ya	Ya

Cipher berdasarkan kebijakan

Tabel berikut menjelaskan cipher yang didukung oleh setiap kebijakan keamanan FIPS.

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-3-FIPS -2023-04 ELBSecurityKebijakan- TLS13 -1-3-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-2-FIPS -2023-04 ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256
ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-1-FIPS -2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan keamanan	Cipher
ELBSecurityKebijakan- TLS13 -1-0-FIPS -2023-04 ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Kebijakan oleh cipher

Tabel berikut menjelaskan kebijakan keamanan FIPS yang mendukung setiap cipher.

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — TLS_AES_128_GCM_ SHA256 IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-3-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-3-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04	1301

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-3-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-3-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04	1302

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
	• ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	
ECDHE-ECDSA-AESOpenSSL - 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c02b

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_DENGAN_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c02f

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL - 128-SHA256 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04	c023

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 128-SHA256 IANA — TLS_ECDHE_RSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c027

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-ECDSA-AES 128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c009
OpenSSL — ECDHE-RSA-AES 128-SHA IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c013

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL - 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c02c

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 256-GCM- SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-RES-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c030

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_256_CBC_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c024

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_RSA_DENGAN_AES_256_CBC_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c028

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-ECDSA-AES 256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	c00a
OpenSSL — ECDHE-RSA-AES 256-SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04	c014

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
AES128OpenSSL — -GCM- SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT0-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	9c
AES128OpenSSL — - SHA256 IANA — TLS_RSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	3c

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — AES128 -SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	2f
AES256OpenSSL — -GCM- SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	9d

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
AES256OpenSSL — - SHA256 IANA — TLS_RSA_DENGAN_AES_256_CBC_ SHA256	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT1-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	3d
OpenSSL — AES256 -SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-2-EXT2-FIPS-PQ-2025-09 • ELBSecurityKebijakan- TLS13 -1-1-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-2023-04 • ELBSecurityKebijakan- TLS13 -1-0-FIPS-PQ-2025-09	35

FS mendukung kebijakan keamanan

Kebijakan keamanan yang didukung FS (Forward Secrecy) memberikan perlindungan tambahan terhadap penyadapan data terenkripsi, melalui penggunaan kunci sesi acak yang unik. Ini mencegah decoding data yang diambil, bahkan jika kunci rahasia jangka panjang dikompromikan.

Kebijakan di bagian ini mendukung FS, dan "FS" disertakan dalam nama mereka. Namun, ini bukan satu-satunya kebijakan yang mendukung FS. Kebijakan yang hanya mendukung TLS 1.3 mendukung FS. Kebijakan yang mendukung TLS 1.3 dan TLS 1.2 yang hanya memiliki cipher dari bentuk TLS_* dan ECDHE_* juga menyediakan FS.

Daftar Isi

Protokol berdasarkan kebijakan

Tabel berikut menjelaskan protokol yang didukung oleh setiap kebijakan keamanan FS yang didukung.

Kebijakan Keamanan	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityKebijakan-FS-1-2-RES-2020-10	Tidak	Ya	Tidak	Tidak
ELBSecurityKebijakan-FS-1-2-RES-2019-08	Tidak	Ya	Tidak	Tidak
ELBSecurityKebijakan-FS-1-2-2019-08	Tidak	Ya	Tidak	Tidak
ELBSecurityKebijakan-FS-1-1-2019-08	Tidak	Ya	Ya	Tidak
ELBSecurityKebijakan-FS-2018-06	Tidak	Ya	Ya	Ya

Cipher berdasarkan kebijakan

Tabel berikut menjelaskan sandi yang didukung oleh setiap kebijakan keamanan yang didukung FS.

Kebijakan keamanan	Cipher
ELBSecurityKebijakan-FS-1-2-RES-2020-10	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384
ELBSecurityKebijakan-FS-1-2-RES-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityKebijakan-FS-1-2-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256
ELBSecurityKebijakan-FS-1-1-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256

Kebijakan keamanan	Cipher
	• ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256
ELBSecurityKebijakan-FS-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256

Kebijakan oleh cipher

Tabel berikut menjelaskan kebijakan keamanan yang didukung FS yang mendukung setiap cipher.

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-ECDSA-AESOpenSSL - 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_128_GCM_ SHA256	• ELBSecurityKebijakan-FS-1-2-RES-2020-10 • ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c02b
ECDHE-RSA-AESOpenSSL - 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_DENGAN_AES_128_GCM_ SHA256	• ELBSecurityKebijakan-FS-1-2-RES-2020-10 • ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c02f
ECDHE-ECDSA-AESOpenSSL - 128-SHA256 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c023
ECDHE-RSA-AESOpenSSL - 128-SHA256	• ELBSecurityKebijakan-FS-1-2-RES-2019-08	c027

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
IANA — TLS_ECDHE_RSA_DENGAN_AES_128_CBC_ SHA256	• ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	
OpenSSL — ECDHE-ECDSA-AES 128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c009
OpenSSL — ECDHE-RSA-AES 128-SHA IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c013
ECDHE-ECDSA-AESOpenSSL - 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_256_GCM_ SHA384	• ELBSecurityKebijakan-FS-1-2-RES-2020-10 • ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c02c

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
ECDHE-RSA-AESOpenSSL - 256-GCM- SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityKebijakan-FS-1-2-RES-2020-10 • ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c030
ECDHE-ECDSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_ECDSA_DENGAN_AES_256_CBC_ SHA384	• ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c024
ECDHE-RSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_RSA_DENGAN_AES_256_CBC_ SHA384	• ELBSecurityKebijakan-FS-1-2-RES-2019-08 • ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c028
OpenSSL — ECDHE-ECDSA-AES 256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c00a

Nama sandi	Kebijakan Keamanan	Rangkaian Penyandian
OpenSSL — ECDHE-RSA-AES 256-SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityKebijakan-FS-1-2-2019-08 • ELBSecurityKebijakan-FS-1-1-2019-08 • ELBSecurityKebijakan-FS-2018-06	c014

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

Saat grup target untuk tindakan default pendengar TCP, TLS, atau QUIC 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.

Pembaruan port untuk pendengar QUIC atau TCP_QUIC tidak diizinkan. Untuk memperbarui port untuk pendengar yang menangani lalu lintas QUIC, pendengar harus dihapus dan dibuat ulang dengan port baru.

Console

Untuk memperbarui pendengar

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 Tindakan, Edit pendengar.
6. Perbarui nilai sesuai kebutuhan.
   - (Opsional) Ubah Protokol.
   - (Opsional) Ubah Port.
   - (Opsional) Pilih grup target yang berbeda untuk tindakan Default.
   - (Opsional) Untuk menambahkan grup target lain, pilih Tambahkan grup target dan perbarui bobot sesuai kebutuhan.
   - (Opsional) Untuk menghapus grup target, pilih Hapus.
7. (Opsional) Tambahkan, perbarui, atau hapus tag sesuai kebutuhan.
8. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui tindakan default

Gunakan perintah modify-listener berikut untuk mengubah grup target.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions Type=forward,TargetGroupArn=new-target-group-arn
```

Contoh berikut memperbarui listener dengan beberapa grup target.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
```

```
            ]
        }
    }]'
```

Untuk menambahkan tag

Gunakan perintah add-tag. Contoh berikut menambahkan dua tag.

```
aws elbv2 add-tags \
    --resource-arns listener-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Untuk menghapus tag

Gunakan perintah remove-tag. Contoh berikut menghapus tag dengan kunci yang ditentukan.

```
aws elbv2 remove-tags \
    --resource-arns listener-arn \
    --tag-keys project department
```

CloudFormation

Untuk memperbarui tindakan default

Perbarui AWS::ElasticLoadBalancingV2::Listenersumber daya untuk menyertakan grup target baru.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref newTargetGroup
```

Atau, untuk mendistribusikan lalu lintas antara beberapa kelompok sasaran, tentukan `DefaultActions` sebagai berikut.

```
DefaultActions:
    - Type: forward
    ForwardConfig:
        TargetGroups:
        - TargetGroupArn: !Ref TargetGroup1
            Weight: 10
        - TargetGroupArn: !Ref TargetGroup2
            Weight: 30
```

Untuk menambahkan tag

Perbarui AWS::ElasticLoadBalancingV2::Listenersumber daya untuk menyertakan properti Tag.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Memperbarui batas waktu idle TCP untuk pendengar Network Load Balancer

Untuk setiap permintaan TCP yang dibuat melalui Network Load Balancer, status koneksi tersebut dilacak. Jika tidak ada data yang dikirim melalui sambungan oleh klien atau target untuk lebih lama dari waktu siaga habis, sambungan ditutup.

Pertimbangan-pertimbangan

- Nilai batas waktu idle default untuk aliran TCP adalah 350 detik.
- Batas waktu idle koneksi untuk pendengar TLS adalah 350 detik dan tidak dapat dimodifikasi.

Console

Untuk memperbarui batas waktu idle TCP

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 Network Load Balancer.
4. Pada tab listeners, pilih kotak centang untuk listener TCP lalu pilih Actions, View listener details.
5. Pada halaman detail pendengar, di tab Atribut, pilih Edit. Jika pendengar menggunakan protokol selain TCP, tab ini tidak ada.
6. Masukkan nilai untuk batas waktu idle TCP dari 60-6000 detik.
7. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui batas waktu idle TCP

Gunakan modify-listener-attributesperintah dengan `tcp.idle_timeout.seconds` atribut.

```
aws elbv2 modify-listener-attributes \
    --listener-arn listener-arn \
    --attributes Key=tcp.idle_timeout.seconds,Value=500
```

Berikut ini adalah output contoh.

```
{
    "Attributes": [
        {
            "Key": "tcp.idle_timeout.seconds",
            "Value": "500"
        }
    ]
}
```

CloudFormation

Untuk memperbarui batas waktu idle TCP

Perbarui AWS::ElasticLoadBalancingV2::Listenersumber daya untuk menyertakan atribut `tcp.idle_timeout.seconds` listener.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      ListenerAttributes:
        - Key: "tcp.idle_timeout.seconds"
          Value: "500"
```

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

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

Mengganti sertifikat default

Anda dapat mengganti sertifikat default untuk pendengar TLS sesuai kebutuhan. Untuk informasi selengkapnya, lihat Sertifikat default.

Console

Untuk mengganti sertifikat default

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Load Balancers.
3. Pilih penyeimbang beban.
4. Pada tab Listeners, pilih teks di kolom Protocol:Port untuk membuka halaman detail untuk listener.
5. Pada tab Sertifikat, pilih Ubah default.
6. Dalam tabel sertifikat ACM dan IAM, pilih sertifikat default baru.
7. (Opsional) Secara default, kami memilih Tambahkan sertifikat default sebelumnya ke daftar sertifikat pendengar. Kami menyarankan agar Anda tetap memilih opsi ini, kecuali saat ini Anda tidak memiliki sertifikat pendengar untuk SNI dan mengandalkan dimulainya kembali sesi TLS.
8. Pilih Simpan sebagai default.

AWS CLI

Untuk mengganti sertifikat default

Gunakan perintah modifikasi-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --certificates CertificateArn=new-default-certificate-arn
```

CloudFormation

Untuk mengganti sertifikat default

Perbarui AWS::ElasticLoadBalancingV2::Listenersumber daya dengan sertifikat default baru.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
```

```
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "new-default-certificate-arn"
```

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 sertifikat default ke daftar sertifikat untuk memastikan bahwa sertifikat ini digunakan dengan protokol SNI meskipun diganti sebagai sertifikat default. Untuk informasi selengkapnya, lihat Daftar sertifikat.

Console

Untuk menambahkan sertifikat ke daftar sertifikat

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 tab Sertifikat.
6. Untuk menambahkan sertifikat default ke daftar, pilih Tambahkan default ke daftar.
7. Untuk menambahkan sertifikat nondefault ke daftar, lakukan hal berikut:

    a. Pilih Tambahkan sertifikat.

    b. Untuk menambahkan sertifikat yang sudah dikelola oleh ACM atau IAM, pilih kotak centang untuk sertifikat dan pilih Sertakan sebagai tertunda di bawah ini.

    c. Untuk menambahkan sertifikat yang tidak dikelola oleh ACM atau IAM, pilih Impor sertifikat, lengkapi formulir, dan pilih Impor.

    d. Pilih Tambahkan sertifikat yang tertunda.

AWS CLI

Untuk menambahkan sertifikat ke daftar sertifikat

Gunakan perintah add-listener-certificates.

```
aws elbv2 add-listener-certificates \
    --listener-arn listener-arn \
    --certificates \
        CertificateArn=certificate-arn-1 \
        CertificateArn=certificate-arn-2 \
        CertificateArn=certificate-arn-3
```

CloudFormation

Untuk menambahkan sertifikat ke daftar sertifikat

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::ListenerCertificate.

```
Resources:
  myCertificateList:
    Type: 'AWS::ElasticLoadBalancingV2::ListenerCertificate'
    Properties:
      ListenerArn: !Ref myTLSListener
      Certificates:
        - CertificateArn: "certificate-arn-1"
        - CertificateArn: "certificate-arn-2"
        - CertificateArn: "certificate-arn-3"

  myTLSListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLSS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn-1"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Menghapus sertifikat dari daftar sertifikat

Anda dapat menghapus sertifikat dari daftar sertifikat untuk pendengar TLS menggunakan prosedur berikut. Setelah Anda menghapus sertifikat, pendengar tidak dapat lagi membuat koneksi menggunakan sertifikat tersebut. Untuk memastikan bahwa klien tidak terpengaruh, tambahkan sertifikat baru ke daftar dan konfirmasikan bahwa koneksi berfungsi sebelum Anda menghapus sertifikat dari daftar.

Untuk menghapus sertifikat default untuk pendengar TLS, lihat Mengganti sertifikat default.

Console

Untuk menghapus sertifikat dari daftar sertifikat

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. Pada tab Sertifikat, pilih kotak centang untuk sertifikat dan pilih Hapus.
6. Saat diminta konfirmasi, masukkan **`confirm`** dan pilih Hapus.

AWS CLI

Untuk menghapus sertifikat dari daftar sertifikat

Gunakan perintah remove-listener-certificates.

```
aws elbv2 remove-listener-certificates \
    --listener-arn listener-arn \
    --certificates CertificateArn=certificate-arn
```

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 Network Load Balancer.

Memperbarui kebijakan keamanan dapat mengakibatkan gangguan jika penyeimbang beban menangani volume lalu lintas yang tinggi. Untuk mengurangi kemungkinan gangguan ketika penyeimbang beban Anda menangani volume lalu lintas yang tinggi, buat penyeimbang beban tambahan untuk membantu menangani lalu lintas atau meminta reservasi LCU.

Console

Untuk memperbarui kebijakan keamanan

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 Tindakan, Edit pendengar.
6. Di bagian Pengaturan pendengar aman, di bawah Kebijakan keamanan, pilih kebijakan keamanan baru.
7. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui kebijakan keamanan

Gunakan perintah modifikasi-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06
```

CloudFormation

Untuk memperbarui kebijakan keamanan

Perbarui AWS::ElasticLoadBalancingV2::Listenersumber daya dengan kebijakan keamanan baru.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "default-certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Memperbarui kebijakan ALPN

Anda dapat memperbarui kebijakan ALPN untuk pendengar TLS sesuai kebutuhan. Untuk informasi selengkapnya, lihat Kebijakan ALPN.

Console

Untuk memperbarui kebijakan ALPN

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 Tindakan, Edit pendengar.
6. Di bagian Pengaturan pendengar aman, untuk kebijakan ALPN, pilih kebijakan untuk mengaktifkan ALPN atau pilih Tidak Ada untuk menonaktifkan ALPN.
7. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui kebijakan ALPN

Gunakan perintah modifikasi-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --alpn-policy HTTP2Preferred
```

CloudFormation

Untuk memperbarui kebijakan ALPN

Perbarui AWS::ElasticLoadBalancingV2::Listenersumber daya untuk menyertakan kebijakan ALPN.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      AlpnPolicy:
        - HTTP2Preferred
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Hapus pendengar untuk Penyeimbang Beban Jaringan Anda

Sebelum Anda menghapus listener, pertimbangkan dampaknya pada aplikasi Anda:

- [Pendengar TCP dan TLS] Penyeimbang beban segera berhenti menerima koneksi baru pada pendengar. Setiap jabat tangan TLS yang sedang berlangsung mungkin gagal. Koneksi yang ada tetap terbuka sampai mereka secara alami menutup atau time out. Permintaan dalam penerbangan pada koneksi yang ada berhasil diselesaikan.
- [Pendengar UDP dan QUIC] Setiap paket dalam perjalanan mungkin tidak mencapai tujuan mereka.

Console

Untuk menghapus pendengar

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.

AWS CLI

Untuk menghapus pendengar

Gunakan perintah hapus-listener.

```
aws elbv2 delete-listener \
    --listener-arn listener-arn
```

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 Penyeimbang Beban Jaringan.

Daftar Isi

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, QUIC, TCP_QUIC
- 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 | TCP_QUIC	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
QUIC	QUIC | TCP_QUIC	instans | ip	HTTP | HTTPS | TCP
TCP_QUIC	TCP_QUIC	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 kelompok target VPC
- 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 Direct Connect atau koneksi Site-to-Site VPN.

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 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 Menggunakan Application Load Balancer sebagai target Network Load Balancer.

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

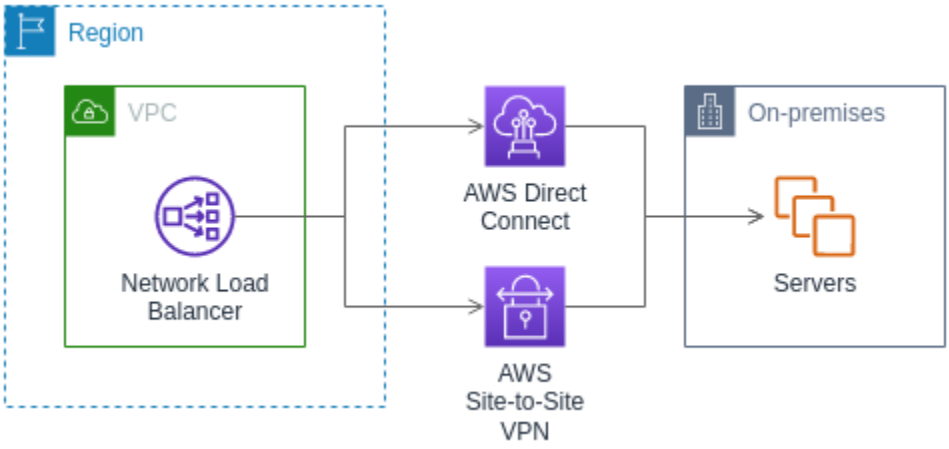
Jika Anda menetapkan target menggunakan ID instans, lalu lintas dialihkan ke instans menggunakan alamat IP privat utama yang ditentukan dalam antarmuka jaringan utama untuk instans. Penyeimbang beban menulis ulang alamat IP tujuan dari paket data sebelum meneruskan ke instans target.

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 Direct Connect atau koneksi Site-to-Site VPN 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 Direct Connect, lihat Apa itu 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.

Grup target untuk Network Load Balancer Anda mendukung jenis alamat IP berikut:

`ipv4`

Penyeimbang beban berkomunikasi dengan target menggunakan. IPv4

`ipv6`

Penyeimbang beban berkomunikasi dengan target menggunakan. IPv6

Pertimbangan-pertimbangan

- Load balancer berkomunikasi dengan target berdasarkan jenis alamat IP dari kelompok target. Target kelompok IPv4 sasaran harus menerima IPv4 lalu lintas dari penyeimbang beban dan target kelompok IPv6 sasaran harus menerima IPv6 lalu lintas dari penyeimbang beban.
- Anda tidak dapat menggunakan grup IPv6 target dengan penyeimbang `ipv4` beban.
- Anda tidak dapat menggunakan grup IPv4 target dengan pendengar UDP untuk penyeimbang `dualstack` beban.
- Anda tidak dapat mendaftarkan Application Load Balancer dengan grup IPv6 target.
- Anda tidak dapat menggunakan grup IPv6 target dengan protokol QUIC atau TCP_QUIC.

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, G1 CC2 CG1, G2 CG2 CR1,,, M1, M2 HI1 HS1, M3, atau T1.
- Saat mendaftarkan target dengan ID instans untuk grup IPv6 target, target harus memiliki IPv6 alamat utama yang ditetapkan. Untuk mempelajari lebih lanjut, lihat IPv6 alamat di Panduan Pengguna Amazon EC2
- Saat mendaftarkan target berdasarkan ID instans, instance harus berada dalam VPC 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 grup target UDP, TCP_UDP, QUIC, dan TCP_QUIC, jangan mendaftarkan instance berdasarkan alamat IP jika mereka berada di luar VPC penyeimbang beban atau jika mereka menggunakan salah satu jenis contoh berikut: C1,,,,,,, G1, G2,,,, M1, M2, M3 CC1 CC2, CG1 atau T1. CG2 CR1 HI1 HS1 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

Anda dapat mengonfigurasi grup target dengan mengedit atributnya. Untuk informasi selengkapnya, lihat Edit 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. Untuk lalu lintas QUIC, nilainya selalu 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`. Atribut ini tidak berlaku untuk lalu lintas QUIC.

`load_balancing.cross_zone.enabled`

Menunjukkan apakah penyeimbangan beban lintas zona diaktifkan. Nilainya adalah`true`, `false` atau`use_load_balancer_configuration`. Nilai default-nya `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, TCP_UDP, QUIC, dan TCP_QUIC.

`proxy_protocol_v2.enabled`

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

`stickiness.enabled`

Menunjukkan apakah sesi lengket diaktifkan. Nilai dari `true` adalah `false`. Default adalah `false`. Atribut ini tidak berlaku untuk lalu lintas QUIC.

`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 meskipun semua target dalam grup target tidak sehat, zona tersebut tidak dihapus dari 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 tersebut 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 meskipun semua target dalam grup target tidak sehat, zona tersebut tidak dihapus dari DNS. Nilai default-nya `off`.

`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. Nilai yang mungkin 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 default adalah 0 detik.

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

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 aplikasi Anda.

Daftar Isi

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.

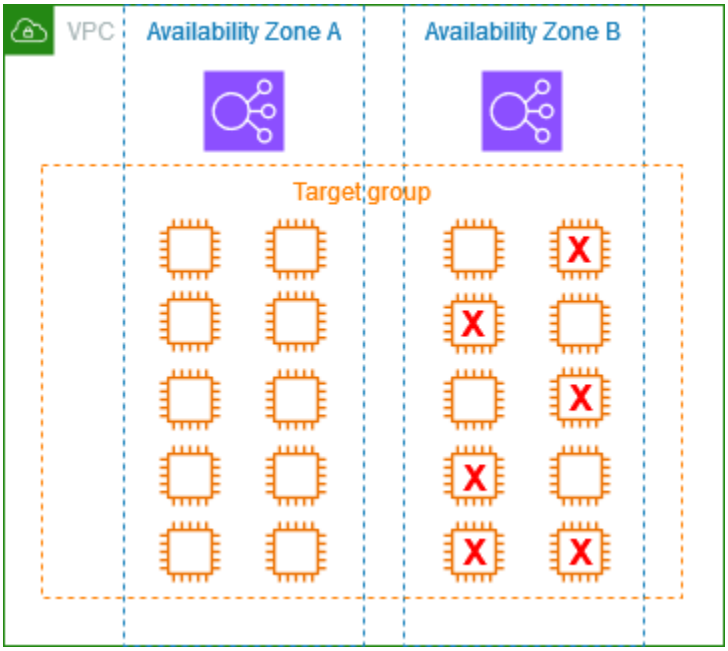
- Ketika failover DNS terjadi, itu berdampak pada semua kelompok target yang terkait dengan penyeimbang beban. Pastikan Anda memiliki kapasitas yang cukup di zona yang tersisa untuk menangani lalu lintas tambahan ini, terutama jika penyeimbangan beban lintas zona tidak aktif.
- Dengan failover DNS, kami menghapus alamat IP 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).
- Dengan failover DNS, jika ada beberapa grup target yang dilampirkan ke Network Load Balancer dan satu grup target tidak sehat di zona, failover DNS terjadi, bahkan jika kelompok target lain sehat di zona itu.
- 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 cukup target sehat 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%
  - Routing failover - 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.

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.

Bagaimana mengevaluasi kesehatan target bekerja

- Jika evaluasi kesehatan target ditetapkan `Yes` pada catatan alias untuk Network Load Balancer, Route 53 mengevaluasi kesehatan sumber daya yang ditentukan oleh nilai. `alias target` Route 53 menggunakan pemeriksaan kesehatan kelompok sasaran.
- Jika semua kelompok sasaran yang dilampirkan ke Network Load Balancer sehat, Route 53 menandai catatan alias sebagai sehat. Jika Anda mengonfigurasi ambang batas untuk grup target dan memenuhi ambang batasnya, itu melewati pemeriksaan kesehatan. Jika tidak, jika kelompok sasaran berisi setidaknya satu target yang sehat, ia melewati pemeriksaan kesehatan. Jika pemeriksaan kesehatan berlalu, Route 53 mengembalikan catatan sesuai dengan kebijakan perutean Anda. Jika kebijakan perutean failover digunakan, Route 53 mengembalikan catatan utama.

- Jika semua grup target yang dilampirkan ke Network Load Balancer tidak sehat, catatan alias gagal dalam pemeriksaan kesehatan Route 53 (fail-open). Jika menggunakan evaluasi kesehatan target, ini menyebabkan kebijakan perutean failover mengarahkan lalu lintas ke sumber daya sekunder.
- Jika semua grup target dalam Network Load Balancer kosong (tidak ada target), Route 53 menganggap catatan tidak sehat (fail-open). Jika menggunakan evaluasi kesehatan target, ini menyebabkan kebijakan perutean failover mengarahkan lalu lintas ke sumber daya sekunder.

Untuk informasi selengkapnya, lihat Menggunakan ambang batas kesehatan grup target penyeimbang beban untuk meningkatkan ketersediaan di AWS Blog dan Mengonfigurasi failover DNS di Panduan Pengembang Amazon Route 53.

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.

Untuk merutekan lalu lintas ke target dalam grup target, membuat pendengar dan menentukan kelompok target dalam tindakan default untuk pendengar. Untuk informasi selengkapnya, lihat Tindakan default. Anda dapat menentukan grup target yang sama di beberapa pendengar, tetapi pendengar ini harus memiliki 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 untuk Network Load Balancer. Anda juga dapat mengubah pengaturan pemeriksaan kesehatan untuk grup target Anda. Untuk informasi selengkapnya, lihat Memperbarui pengaturan pemeriksaan kesehatan dari grup target Network Load Balancer.

Persyaratan

- Setelah Anda membuat grup target, Anda tidak dapat mengubah jenis target atau jenis alamat IP-nya.
- Semua target dalam grup target harus memiliki jenis alamat IP yang sama dengan grup target: IPv4 atau IPv6.
- Anda harus menggunakan grup IPv6 target dengan penyeimbang beban dualstack.

- Anda tidak dapat menggunakan grup IPv4 target dengan pendengar UDP untuk penyeimbang `dualstack` beban.
- Anda tidak dapat menggunakan grup IPv6 target dengan protokol QUIC atau TCP_QUIC.

Console

Untuk membuat grup target

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.
      - Jika protokol pendengar adalah QUIC, pilih QUIC.
      - Jika protokol pendengar adalah TCP_QUIC, pilih TCP_QUIC.
      - Jika jenis targetnya adalah Application Load Balancer, protokolnya harus TCP.
   d. Untuk Port, ubah nilai default sesuai kebutuhan.

      Jika jenis targetnya adalah Application Load Balancer, port harus cocok dengan port listener Application Load Balancer.
   e. Untuk jenis alamat IP, pilih IPv4atau IPv6. Opsi ini hanya tersedia jika jenis targetnya adalah Instans atau alamat IP.

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 ???.
6. (Opsional) Untuk menambahkan tag, perluas Tag, pilih Tambahkan tag, dan masukkan kunci tag dan nilai tag.
7. Pilih Berikutnya.
8. (Opsional) Daftarkan target. Jenis target dari kelompok sasaran menentukan informasi yang Anda berikan. Jika Anda belum siap untuk mendaftarkan target sekarang, Anda dapat mendaftarkannya nanti.
   - Instans — Pilih instans EC2, masukkan port, dan pilih Sertakan sebagai tertunda di bawah ini.
   - Alamat IP — Pilih VPC yang berisi alamat IP atau alamat IP pribadi lainnya, masukkan alamat IP dan port, dan pilih Sertakan sebagai tertunda di bawah ini.
   - Application Load Balancer — Pilih Application Load Balancer. Untuk informasi selengkapnya, lihat Gunakan Application Load Balancers sebagai target.
9. PilihBuat grup target.

AWS CLI

Untuk membuat grup target

Gunakan perintah create-target-group. Contoh berikut membuat grup target dengan protokol TCP, target yang terdaftar berdasarkan alamat IP, satu tag, dan pengaturan pemeriksaan kesehatan default.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type ip \
    --vpc-id vpc-1234567890abcdef0 \
```

```
    --tags Key=department,Value=123
```

Untuk mendaftarkan target

Gunakan perintah register-target untuk mendaftarkan target dengan kelompok target. Sebagai contoh, lihat the section called “Daftarkan target”.

CloudFormation

Untuk membuat grup target

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::TargetGroup. Contoh berikut membuat grup target dengan protokol TCP, target yang terdaftar berdasarkan alamat IP, satu tag, pengaturan pemeriksaan kesehatan default, dan dua target terdaftar.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: 10.0.50.10
          Port: 80
        - Id: 10.0.50.20
          Port: 80
```

Memperbarui pengaturan kesehatan grup target untuk Network Load Balancer

Secara default, Network Load Balancer memantau kesehatan target dan merutekan permintaan ke target yang sehat. Namun, jika penyeimbang beban tidak memiliki target yang cukup sehat, maka secara otomatis mengirimkan lalu lintas ke semua target yang terdaftar (gagal terbuka). Anda dapat mengubah pengaturan kesehatan grup target untuk grup target Anda untuk menentukan ambang

batas untuk failover DNS dan failover routing. Untuk informasi selengkapnya, lihat the section called “Kesehatan kelompok sasaran”.

Console

Untuk memperbarui pengaturan kesehatan grup target

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. Perluas persyaratan kesehatan kelompok sasaran.
6. Untuk jenis Konfigurasi, sebaiknya pilih Konfigurasi terpadu, yang menetapkan ambang batas yang sama untuk failover DNS dan failover routing.
7. 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.
8. Teks informasi menunjukkan apakah penyeimbangan beban lintas zona diaktifkan untuk grup target. Jika penyeimbangan beban lintas zona dinonaktifkan, Anda dapat mengaktifkannya untuk memastikan bahwa Anda memiliki kapasitas yang cukup. Di bawah Konfigurasi pemilihan Target, perbarui penyeimbangan beban lintas zona.

   Teks berikut menunjukkan bahwa penyeimbangan beban lintas zona dinonaktifkan:

   ```
   Healthy state requirements apply to each zone independently.
   ```

   Teks berikut menunjukkan bahwa penyeimbangan beban lintas zona diaktifkan:

   ```
   Healthy state requirements apply to the total targets across all applicable
    zones.
   ```
9. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui pengaturan kesehatan grup target

Gunakan perintah modify-target-group-attributes. 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 target-group-arn \
    --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=5
```

CloudFormation

Untuk mengubah pengaturan kesehatan kelompok sasaran

Perbarui AWS::ElasticLoadBalancingV2::TargetGroupsumber daya. Contoh berikut menetapkan ambang batas yang sehat untuk kedua tindakan negara yang tidak sehat menjadi 50%.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - 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"
```

Pemeriksaan kondisi untuk grup target Penyeimbang Beban Jaringan

Anda mendaftarkan target Anda dengan satu atau lebih grup target. Penyeimbang beban mulai mengarahkan permintaan ke target yang baru terdaftar segera setelah proses pendaftaran selesai

dan target lulus pemeriksaan kesehatan awal. 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 dan QUIC, ketersediaan target dapat diuji menggunakan pemeriksaan kesehatan non-UDP pada kelompok sasaran Anda. Anda dapat menggunakan pemeriksaan kesehatan apa pun yang tersedia (TCP, HTTP, atau HTTPS), dan port apa pun pada target Anda untuk memverifikasi ketersediaan layanan Anda. Jika layanan yang menerima pemeriksaan kesehatan gagal, target Anda dianggap tidak tersedia. Untuk meningkatkan akurasi pemeriksaan kesehatan untuk layanan Anda, konfigurasikan layanan mendengarkan port pemeriksaan kesehatan untuk melacak status layanan UDP atau QUIC Anda dan gagal pemeriksaan kesehatan jika layanan tidak tersedia.

Untuk informasi selengkapnya, lihat the section called “Kesehatan kelompok sasaran”.

Daftar Isi

Pengaturan pemeriksaan kesehatan

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

Pengaturan	Deskripsi	Default
HealthCheckProtocol	Protokol penyeimbang beban gunakan saat melakukan pemeriksaan kesehatan pada target. Protokol yang mungkin adalah HTTP, HTTPS, dan TCP. Default-nya adalah protokol TCP. Jika jenis targetnya adalah`alb`, protokol	TCP

Pengaturan	Deskripsi	Default
	pemeriksaan kesehatan yang didukung adalah HTTP dan HTTPS.	
HealthCheckPort	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 penyeimbang beban.
HealthCheckPath	[Pemeriksaan kesehatan HTTP/HTTPS] Jalur pemeriksaan kesehatan yang menjadi tujuan pada target pemeriksaan kesehatan. Default-nya 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. Pemeriksaan Kesehatan untuk Penyeimba ng Beban Jaringan didistribusikan dan menggunakan mekanisme konsensus untuk menentukan target kesehatan. Oleh karena itu, target menerima lebih dari jumlah dikonfigurasi 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 pemeriksaan kesehatan TCP.	30 detik
HealthyThresholdCount	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
UnhealthyThresholdCount	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
Pencocokan	[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.RegistrationInProgress` | `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. 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`

Nilai	Deskripsi
`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
`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

Kode alasan	Deskripsi
	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 Network Load Balancer Anda

Anda dapat memeriksa status kondisi target yang terdaftar dengan kelompok target Anda. Untuk bantuan dengan kegagalan pemeriksaan kesehatan, lihat Pemecahan masalah: Target terdaftar tidak dalam layanan.

Console

Untuk memeriksa kesehatan target Anda

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. Tab 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 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.

AWS CLI

Untuk memeriksa kesehatan target Anda

Gunakan perintah describe-target-health. Contoh ini memfilter output untuk memasukkan hanya target yang tidak sehat. Untuk target yang tidak sehat, outputnya menyertakan kode alasan.

```
aws elbv2 describe-target-health \
    --target-group-arn target-group-arn \
    --query "TargetHealthDescriptions[?TargetHealth.State!='healthy'].
[Target.Id,TargetHealth.State,TargetHealth.Reason]" \
    --output table
```

Berikut ini adalah output contoh.

```
-----------------------------------------------
|            DescribeTargetHealth             |
+--------------+---------+--------------------+
|  172.31.0.57 |  unused |  Target.NotInUse   |
|  172.31.0.50 |  unused |  Target.NotInUse   |
+--------------+---------+--------------------+
```

Status target dan kode alasan

Daftar berikut menunjukkan kode alasan yang mungkin untuk setiap status target.

Target state adalah healthy

Kode alasan tidak disediakan.

Target state adalah initial

- `Elb.RegistrationInProgress`- Targetnya sedang dalam proses didaftarkan pada load balancer.
- `Elb.InitialHealthChecking`- Load balancer masih mengirimkan target jumlah minimum pemeriksaan kesehatan yang diperlukan untuk menentukan status kesehatannya.

Target state adalah unhealthy

- `Target.FailedHealthChecks`- Penyeimbang beban menerima kesalahan saat membuat koneksi ke target atau respons target salah bentuk.

Target state adalah unused

- `Target.NotRegistered`- Target tidak terdaftar dengan kelompok sasaran.
- `Target.NotInUse`- Grup sasaran tidak digunakan oleh penyeimbang beban atau target berada di Availability Zone yang tidak diaktifkan untuk penyeimbang muatannya.
- `Target.InvalidState`- Target dalam keadaan berhenti atau dihentikan.
- `Target.IpUnusable`- Alamat IP target dicadangkan untuk digunakan oleh penyeimbang beban.

Target state adalah draining

- `Target.DeregistrationInProgress`- Target sedang dalam proses dideregistrasi dan periode penundaan deregistrasi belum kedaluwarsa.

Target state adalah unavailable

- `Elb.InternalError`- Kesehatan target tidak tersedia karena kesalahan internal.

Memperbarui pengaturan pemeriksaan kesehatan dari grup target Network Load Balancer

Anda dapat memperbarui pengaturan pemeriksaan kesehatan untuk grup target Anda kapan saja. Untuk daftar pengaturan pemeriksaan kesehatan, lihatthe section called “Pengaturan pemeriksaan kesehatan”.

Console

Untuk memperbarui pengaturan pemeriksaan kesehatan

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 Edit pengaturan pemeriksaan kesehatan, ubah pengaturan sesuai kebutuhan.
6. Pilih Simpan perubahan.

AWS CLI

Untuk memperbarui pengaturan pemeriksaan kesehatan

Gunakan perintah modify-target-group. Contoh berikut memperbarui HealthyThresholdCountdan HealthCheckTimeoutSecondspengaturan.

```
aws elbv2 modify-target-group \
    --target-group-arn target-group-arn \
    --healthy-threshold-count 3 \
    --health-check-timeout-seconds 20
```

CloudFormation

Untuk memperbarui pengaturan pemeriksaan kesehatan

Perbarui AWS::ElasticLoadBalancingV2::TargetGroupsumber daya untuk menyertakan pengaturan pemeriksaan kesehatan yang diperbarui. Contoh berikut memperbarui HealthyThresholdCountdan HealthCheckTimeoutSecondspengaturan.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      HealthyThresholdCount: 3
      HealthCheckTimeoutSeconds: 20
```

Mengedit atribut grup target untuk Network Load Balancer

Setelah membuat grup target untuk Network Load Balancer, Anda dapat mengedit atribut grup targetnya.

Atribut grup target

- Preservasi IP klien
- Penundaan Pembatalan Pendaftaran

- Protokol proxy
- Sesi lengket
- Penyeimbangan beban lintas zona untuk kelompok sasaran
- Pengakhiran koneksi untuk target yang tidak sehat
- Interval pengeringan yang tidak sehat

Preservasi IP klien

Network Load Balancers dapat mempertahankan alamat IP sumber klien saat merutekan permintaan ke target backend. Saat Anda menonaktifkan pelestarian IP klien, alamat IP sumber adalah alamat IP pribadi dari Network Load Balancer.

Secara default, pelestarian IP klien diaktifkan (dan tidak dapat dinonaktifkan) misalnya dan grup target tipe IP dengan protokol UDP, TCP_UDP, QUIC, dan TCP_QUIC. 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, QUIC, TCP_QUIC): Diaktifkan
- Grup target tipe IP (TCP, TLS): Dinonaktifkan

Saat pelestarian IP klien diaktifkan

Tabel berikut menjelaskan alamat IP yang ditargetkan menerima ketika pelestarian IP klien diaktifkan.

Target	IPv4 permintaan klien	IPv6 permintaan klien
Jenis contoh (IPv4)	IPv4 Alamat klien	Alamat penyeimbang IPv4 beban
Jenis IP (IPv4)	IPv4 Alamat klien	Alamat penyeimbang IPv4 beban
Jenis IP (IPv6)	Alamat penyeimbang IPv6 beban	IPv6 Alamat klien

Ketika pelestarian IP klien dinonaktifkan

Tabel berikut menjelaskan alamat IP yang ditargetkan menerima ketika pelestarian IP klien dinonaktifkan.

Target	IPv4 permintaan klien	IPv6 permintaan klien
Jenis contoh (IPv4)	Alamat penyeimbang IPv4 beban	Alamat penyeimbang IPv4 beban
Jenis IP (IPv4)	Alamat penyeimbang IPv4 beban	Alamat penyeimbang IPv4 beban
Jenis IP (IPv6)	Alamat penyeimbang IPv6 beban	Alamat penyeimbang IPv6 beban

Persyaratan dan pertimbangan

- Perubahan pelestarian klien IP berlaku hanya untuk koneksi TCP baru.
- Ketika pelestarian IP klien diaktifkan, lalu lintas harus mengalir langsung dari Network Load Balancer ke target. Target harus berada di VPC yang sama dengan penyeimbang beban atau di VPC peered di Wilayah yang sama.
- Pelestarian IP klien tidak didukung ketika target dicapai melalui gateway transit.
- Pelestarian IP klien tidak didukung saat menggunakan titik akhir Load Balancer Gateway untuk memeriksa lalu lintas antara Network Load Balancer dan target (contoh atau alamat IP), meskipun target berada dalam VPC yang sama dengan Network Load Balancer.
- Jenis contoh berikut tidak mendukung pelestarian IP klien: C1,,,,, CC1, CC2 CG1, G1 CG2 CR1, G2,,, M1 HI1, M2 HS1, 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. Alamat IP sumber AWS PrivateLink lalu lintas selalu merupakan alamat IP pribadi dari Network Load Balancer.
- Pelestarian IP klien tidak didukung ketika grup target berisi antarmuka AWS PrivateLink jaringan, atau antarmuka jaringan Network Load Balancer lain. Hal ini menyebabkan hilangnya komunikasi dengan target tersebut.

- Pelestarian IP klien tidak berpengaruh pada lalu lintas yang dikonversi dari IPv6 ke IPv4. Alamat IP sumber dari jenis lalu lintas ini selalu merupakan alamat IP pribadi dari Network Load Balancer.
- 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.
- Loopback NAT, juga dikenal sebagai hairpinning, tidak didukung saat pelestarian IP klien diaktifkan. Hal ini terjadi ketika menggunakan Network Load Balancer internal, dan target yang terdaftar di belakang Network Load Balancer membuat koneksi ke Network Load Balancer yang sama. Koneksi dapat diarahkan ke target yang mencoba membuat koneksi, yang menyebabkan kesalahan koneksi. Kami menyarankan untuk tidak menghubungkan ke Network Load Balancer dari target di belakang Network Load Balancer yang sama, atau Anda juga dapat mencegah jenis kesalahan koneksi ini dengan menonaktifkan pelestarian IP klien. Jika Anda memerlukan alamat IP klien, Anda dapat menggunakan mengambilnya menggunakan Proxy Protocol v2. Untuk informasi selengkapnya, lihat Protokol proxy.
- 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. Untuk informasi selengkapnya, lihat Kesalahan alokasi port untuk aliran backend.

Console

Untuk memodifikasi pelestarian IP klien

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 laman detailnya.
4. Pada tab Atribut, pilih Edit dan temukan panel konfigurasi Lalu lintas.
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.

AWS CLI

Untuk mengaktifkan pelestarian IP klien

Gunakan modify-target-group-attributesperintah dengan `preserve_client_ip.enabled` atribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=preserve_client_ip.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan pelestarian IP klien

Perbarui AWS::ElasticLoadBalancingV2::TargetGroup sumber daya untuk menyertakan `preserve_client_ip.enabled` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "preserve_client_ip.enabled"
          Value: "true"
```

Penundaan Pembatalan Pendaftaran

Ketika target dideregistrasi, 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 target deregistering adalah`draining`, di mana target akan berhenti menerima koneksi baru. Namun, target mungkin masih menerima koneksi karena penundaan propagasi konfigurasi. 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. Untuk lalu lintas QUIC nilainya selalu 300 detik, dan tidak dapat disesuaikan.

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

Console

Untuk memodifikasi atribut penundaan deregistrasi

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 laman 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.

AWS CLI

Untuk memodifikasi atribut penundaan deregistrasi

Gunakan modify-target-group-attributesperintah dengan `deregistration_delay.connection_termination.enabled` atribut `deregistration_delay.timeout_seconds` dan.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \
      "Key=deregistration_delay.timeout_seconds,Value=60" \
      "Key=deregistration_delay.connection_termination.enabled,Value=true"
```

CloudFormation

Untuk memodifikasi atribut penundaan deregistrasi

Perbarui AWS::ElasticLoadBalancingV2::TargetGroupsumber daya untuk menyertakan `deregistration_delay.timeout_seconds` dan `deregistration_delay.connection_termination.enabled` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "deregistration_delay.timeout_seconds"
          Value: "60"
        - Key: "deregistration_delay.connection_termination.enabled"
          Value: "true"
```

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 Network Load Balancer Anda, header protokol proxy pertama mungkin bukan yang dari penyeimbang beban.

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

Lalu lintas QUIC tidak mendukung protokol proxy versi 2.

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: Secara default, pelestarian IP klien dinonaktifkan, dan alamat IP sumber yang diberikan ke aplikasi Anda adalah alamat IP pribadi dari node penyeimbang beban. Untuk mempertahankan alamat IP klien, pastikan bahwa target berada dalam VPC yang sama atau VPC peered dan aktifkan pelestarian IP klien. Jika Anda memerlukan alamat IP klien dan kondisi ini tidak terpenuhi, aktifkan protokol proxy dan dapatkan alamat IP klien dari header protokol proxy.
- UDP dan TCP_UDP: Alamat IP sumber adalah alamat IP klien, karena pelestarian IP klien diaktifkan secara default untuk protokol ini dan tidak dapat dinonaktifkan. 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.

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.

Target dapat gagal pemeriksaan kesehatan jika mereka tidak dapat mengurai header protokol proxy. Misalnya, mereka mungkin mengembalikan kesalahan berikut: HTTP 400: Permintaan buruk.

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 vektor kustom Type-Length-Value (TLV) sebagai berikut.

Bidang	Panjang (dalam oktet)	Deskripsi
Jenis	1	PP2_TYPE_AWS (0xEA)

Bidang	Panjang (dalam oktet)	Deskripsi
Panjangnya	2	Panjang nilai
Nilai	1	PP2_subtipe_ AWS_VPCE_ID (0x01)
	variabel (nilai panjang dikurangi 1)	ID dari titik akhir

Untuk contoh yang mem-parsing tipe TLV 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.

Console

Untuk mengaktifkan protokol proxy versi 2

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.

AWS CLI

Untuk mengaktifkan protokol proxy versi 2

Gunakan modify-target-group-attributesperintah dengan `proxy_protocol_v2.enabled` atribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=proxy_protocol_v2.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan protokol proxy versi 2

Perbarui AWS::ElasticLoadBalancingV2::TargetGroup sumber daya untuk menyertakan `proxy_protocol_v2.enabled` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "proxy_protocol_v2.enabled"
          Value: "true"
```

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-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 atau QUIC.

Console

Untuk mengaktifkan sesi lengket

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 laman detailnya.
4. Pada tab Atribut, pilih Edit.
5. Di bawah Konfigurasi pemilihan target, aktifkan Stickiness.
6. Pilih Simpan perubahan.

AWS CLI

Untuk mengaktifkan sesi lengket

Gunakan modify-target-group-attributesperintah dengan `stickiness.enabled` atribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=stickiness.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan sesi lengket

Perbarui AWS::ElasticLoadBalancingV2::TargetGroup sumber daya untuk menyertakan `stickiness.enabled` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "stickiness.enabled"
          Value: "true"
```

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 yang 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 mengaktifkannya 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-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.
- Ketika penyeimbangan beban lintas zona dinonaktifkan, 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 dinonaktifkan, pastikan bahwa semua grup target berpartisipasi dalam Availability Zone yang sama. Availability Zone yang kosong dianggap tidak sehat.
- Anda dapat mengaktifkan atau menonaktifkan penyeimbangan beban lintas zona di tingkat grup target jika jenis 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 informasi selengkapnya tentang mengaktifkan penyeimbangan beban lintas zona pada tingkat penyeimbang beban, lihat. the section called “Penyeimbangan beban lintas zona”

Console

Untuk mengaktifkan penyeimbangan beban lintas zona untuk grup target

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.

AWS CLI

Untuk mengaktifkan penyeimbangan beban lintas zona untuk grup target

Gunakan modify-target-group-attributesperintah dengan `load_balancing.cross_zone.enabled` atribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Untuk mengaktifkan penyeimbangan beban lintas zona untuk grup target

Perbarui AWS::ElasticLoadBalancingV2::TargetGroup sumber daya untuk menyertakan `load_balancing.cross_zone.enabled` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
```

```
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Pengakhiran koneksi untuk target yang tidak sehat

Pengakhiran 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 dikonfigurasi pada tingkat kelompok target.

Console

Untuk memodifikasi atribut penghentian koneksi

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.

AWS CLI

Untuk menonaktifkan atribut penghentian koneksi

Gunakan modify-target-group-attributesperintah dengan `target_health_state.unhealthy.connection_termination.enabled` atribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.connection_termination.enabled,Value=false"
```

CloudFormation

Untuk menonaktifkan atribut penghentian koneksi

Perbarui AWS::ElasticLoadBalancingV2::TargetGroup sumber daya untuk menyertakan `target_health_state.unhealthy.connection_termination.enabled` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.connection_termination.enabled"
          Value: "false"
```

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, kondisinya menjadi `healthy` lagi. Jika deregistrasi dipicu, status target menjadi `draining` dan batas waktu tunda deregistrasi dimulai.

Persyaratan

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

Console

Untuk memodifikasi interval pengeringan yang tidak sehat

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.

AWS CLI

Untuk memodifikasi interval pengeringan yang tidak sehat

Gunakan modify-target-group-attributesperintah dengan `target_health_state.unhealthy.draining_interval_seconds` atribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.draining_interval_seconds,Value=60"
```

CloudFormation

Untuk memodifikasi interval pengeringan yang tidak sehat

Perbarui AWS::ElasticLoadBalancingV2::TargetGroup sumber daya untuk menyertakan `target_health_state.unhealthy.draining_interval_seconds` atribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.draining_interval_seconds"
          Value: "60"
```

Daftarkan target untuk Network Load Balancer

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 instance IDs, 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 Penyeimbang Beban Jaringan.

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 Pembatalan Pendaftaran.

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.

Daftar Isi

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, pelestarian alamat IP klien tidak berfungsi saat menerjemahkan IPv4 alamat ke, atau ke

IPv6 alamat. IPv6 IPv4 Pelestarian alamat IP klien hanya berfungsi ketika alamat IP klien dan target keduanya IPv4 atau keduanya IPv6.

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 IPv4 Alamat pribadi.

Untuk informasi selengkapnya, lihat Memperbarui grup keamanan untuk Network Load Balancer.

Jaringan ACLs

Saat Anda mendaftarkan instans EC2 sebagai target, Anda harus memastikan bahwa jaringan ACLs untuk subnet untuk instans Anda memungkinkan lalu lintas di port pendengar dan port pemeriksaan kesehatan. Daftar kontrol akses jaringan (ACL) default untuk VPC memungkinkan semua lalu lintas masuk dan keluar. Jika Anda membuat jaringan khusus ACLs, verifikasi bahwa mereka mengizinkan lalu lintas yang sesuai.

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

Aturan yang disarankan untuk subnet instans

Inbound

Sumber	Protokol	Rentang Port	Komentar
Client IP addresses	*listener*	*target port*	Izinkan lalu lintas klien (IP Preservation:ON)
VPC CIDR	*listener*	*target port*	Izinkan lalu lintas klien (IP Preservation:OFF)
VPC CIDR	*health check*	*health check*	Izinkan lalu lintas pemeriksaan kesehatan

Outbound

Tujuan	Protokol	Rentang Port	Komentar
Client IP addresses	*listener*	1024-65535	Izinkan lalu lintas kembali ke klien (IP Preservation:0N)
VPC CIDR	*listener*	1024-65535	Izinkan lalu lintas kembali ke klien (IP Preservation:0FF)
VPC CIDR	*health check*	1024-65535	Izinkan lalu lintas pemeriksaan kesehatan

Jaringan yang ACLs terkait dengan subnet untuk penyeimbang beban Anda harus memungkinkan lalu lintas berikut untuk penyeimbang beban yang menghadap ke internet.

Aturan yang disarankan untuk subnet penyeimbang beban

Inbound

Sumber	Protokol	Rentang Port	Komentar
Client IP addresses	*listener*	*listener*	Izinkan lalu lintas klien
VPC CIDR	*listener*	1024-65535	Izinkan respons dari target
VPC CIDR	*health check*	1024-65535	Izinkan lalu lintas pemeriksaan kesehatan

Outbound

Tujuan	Protokol	Rentang Port	Komentar

Client IP addresses	*listener*	1024-65535	Izinkan tanggapan terhadap klien
VPC CIDR	*listener*	*target port*	Izinkan permintaan ke target
VPC CIDR	*health check*	*health check*	Izinkan pemeriksaan kesehatan ke target

Untuk penyeimbang beban internal, jaringan ACLs untuk subnet untuk instance dan node penyeimbang beban Anda harus mengizinkan lalu lintas masuk dan keluar ke dan dari CIDR VPC, pada port pendengar dan port singkat.

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 (Hong Kong) `ap-east-1`
- Timur Tengah (Bahrain) `me-south-1`
- AWS Tiongkok (Beijing) `cn-north-1`
- AWS Tiongkok (Ningxia) `cn-northwest-1`

Daftarkan target

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

Jenis target grup target Anda menentukan target mana yang dapat Anda daftarkan. Untuk informasi selengkapnya, lihat Jenis target. Gunakan informasi di bawah ini untuk mendaftarkan target dengan jenis kelompok sasaran `instance` atau`ip`. Jika jenis targetnya adalah`alb`, lihatGunakan Application Load Balancers sebagai target.

Persyaratan dan pertimbangan

- Suatu instans harus berada di negara `running` saat Anda mendaftarkannya.
- Anda tidak dapat mendaftarkan instance berdasarkan ID instans jika menggunakan salah satu jenis instance berikut: C1,,,,, CC1, G1 CC2 CG1, G2 CG2 CR1,,, M1, M2 HI1 HS1, M3, atau T1.
- Saat mendaftarkan target berdasarkan ID instans, instance harus berada dalam VPC 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.
- Saat mendaftarkan target dengan ID instans untuk grup IPv6 target, target harus memiliki IPv6 alamat utama yang ditetapkan. Untuk mempelajari selengkapnya, lihat IPv6 alamat di Panduan Pengguna Amazon EC2
- Saat mendaftarkan target berdasarkan alamat IP untuk grup IPv4 target, alamat IP yang Anda daftarkan harus berasal dari salah satu blok CIDR berikut:
  - Subnet dari kelompok target VPC
  - 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)
- Saat mendaftarkan target berdasarkan alamat IP untuk grup IPv6 target, alamat IP yang Anda daftarkan harus berada di dalam blok CIDR VPC atau di dalam blok IPv6 CIDR dari VPC IPv6 peered.
- 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 grup target UDP, TCP_UDP, QUIC, dan TCP_QUIC, jangan mendaftarkan instance berdasarkan alamat IP jika mereka berada di luar VPC penyeimbang beban atau jika mereka menggunakan salah satu jenis contoh berikut: C1,,,,,,, G1, G2,,,, M1, M2, M3 CC1 CC2, CG1 atau T1. CG2 CR1 HI1 HS1 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.

Persyaratan dan pertimbangan khusus QUIC

- Semua target yang terdaftar ke grup target QUIC atau TCP_QUIC harus memiliki ID server yang ditentukan.
- Server IDs harus unik untuk semua target yang ada dalam pendengar Network Load Balancer.
- Server QUIC IDs selalu 8 byte. Saat mendaftarkan target, ID server harus dalam bentuk `0x` diikuti oleh 16 karakter heksadesimal.
- Setelah target terdaftar dengan ID server, ID tersebut tidak dapat diubah. Untuk mengubah ID server target, itu harus dideregistrasi terlebih dahulu dan kemudian terdaftar dengan ID server baru.
- Pengidentifikasi target dan kombinasi port harus memiliki satu ID server. Menggunakan ID server yang berbeda untuk IP atau ID instance dan kombinasi port yang sama dalam VPC yang sama tidak didukung.
- Hindari menggunakan kembali ID server yang sama untuk target yang berbeda dalam waktu 6 jam.

Console

Untuk mendaftarkan target

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. Pilih Daftarkan target.
6. Jika jenis target grup target adalah`instance`, pilih instance yang tersedia, ganti port default jika diperlukan, lalu pilih Sertakan sebagai tertunda di bawah ini.
7. Jika jenis target grup target adalah`ip`, untuk setiap alamat IP, pilih jaringan, masukkan alamat IP dan port, dan pilih Sertakan sebagai tertunda di bawah ini.
8. Jika tipe target dari grup target adalah`alb`, ganti port default jika diperlukan dan pilih Application Load Balancer. Untuk informasi selengkapnya, lihat Gunakan Application Load Balancers sebagai target.
9. Jika protokol grup target adalah QUIC atau TCP_QUIC, pastikan ID server ditentukan.
10. Pilih Daftarkan target yang tertunda.

AWS CLI

Untuk mendaftarkan target

Gunakan perintah register-target. Contoh berikut mendaftarkan target dengan ID instance. Karena port tidak ditentukan, penyeimbang beban menggunakan port grup target.

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

Contoh berikut mendaftarkan target dengan alamat IP. Karena port tidak ditentukan, penyeimbang beban menggunakan port grup target.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10 Id=10.0.50.20
```

Contoh berikut mendaftarkan Application Load Balancer sebagai target.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=application-load-balancer-arn
```

Contoh berikut mendaftarkan target ke dalam kelompok target QUIC atau TCP_QUIC.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10,QuicServerId=0xa1b2c3d4e5f65890
 Id=10.0.50.20,QuicServerId=0xa1b2c3d4e5f65999
```

CloudFormation

Untuk mendaftarkan target

Perbarui AWS::ElasticLoadBalancingV2::TargetGroupsumber daya untuk memasukkan target baru. Contoh berikut mendaftarkan dua target dengan ID instance.

```
Resources:
  myTargetGroup:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
```

Contoh berikut mendaftarkan dua target dengan ID instance ke grup target protokol QUIC atau TCP_QUIC.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65999
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65000
```

Target deregister

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.

Console

Untuk membatalkan pendaftaran target

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 laman detailnya.
4. Pada tab Target, pilih target yang akan dihapus.
5. Pilih Batalkan pendaftaran.

AWS CLI

Untuk membatalkan pendaftaran target

Gunakan perintah Target deregister. Contoh berikut deregister dua target yang terdaftar oleh ID instance.

```
aws elbv2 deregister-targets \
    --target-group-arn target-group-arn \
    --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

Menggunakan Application Load Balancer sebagai target Network Load Balancer

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-pertimbangan

- Anda hanya dapat mendaftarkan satu Application Load Balancer per grup target.
- Untuk mengaitkan Application Load Balancer sebagai target Network Load Balancer, load balancer harus berada dalam VPC yang sama dalam akun yang sama.
- Anda dapat mengaitkan Application Load Balancer sebagai target hingga dua Network Load Balancer. Untuk melakukan ini, daftarkan Application Load Balancer dengan kelompok target terpisah untuk setiap Network Load Balancer.
- Setiap Application Load Balancer yang Anda daftarkan dengan Network Load Balancer mengurangi jumlah maksimum target per Availability Zone per Network Load Balancer sebesar 50. 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.
- Komunikasi antara Network Load Balancer dan Application Load Balancer selalu menggunakan. IPv4

Tugas

- Prasyarat
- Langkah 1: Buat kelompok target dari jenis alb
- Langkah 2: Buat Network Load Balancer dan konfigurasikan routing
- Langkah 3: (Opsional) Buat layanan titik akhir VPC

Prasyarat

Jika Anda belum memiliki Application Load Balancer untuk digunakan sebagai target, buat penyeimbang beban, pendengarnya, dan grup targetnya. Untuk informasi selengkapnya, lihat Membuat Application Load Balancer di Panduan Pengguna untuk Application Load Balancers.

Langkah 1: Buat kelompok target dari jenis alb

Buat kelompok target tipe`alb`. Anda dapat mendaftarkan Application Load Balancer sebagai target saat Anda membuat grup target atau nanti.

Console

Untuk membuat grup target untuk Application Load Balancer sebagai target

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. Di panel konfigurasi Dasar, untuk Pilih jenis target, pilih Application Load Balancer.
5. Untuk Name, masukkan nama untuk grup target.
6. Untuk Protokol, hanya TCP yang diizinkan. Pilih Port untuk grup target Anda. Port untuk grup target ini harus sesuai dengan port listener Application Load Balancer. Jika Anda memilih port yang berbeda untuk grup target ini, Anda dapat memperbarui port listener pada Application Load Balancer agar sesuai dengannya.
7. Untuk VPC, pilih virtual private cloud (VPC) untuk grup target. Ini harus VPC yang sama yang digunakan oleh Application Load Balancer.
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) Perluas Tag. Untuk setiap tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
10. Pilih Berikutnya.
11. Jika Anda siap untuk mendaftarkan Application Load Balancer, pilih Register now, override port default jika diperlukan, dan pilih Application Load Balancer. Application Load Balancer harus memiliki listener pada port yang sama dengan kelompok target. Anda dapat menambahkan atau mengedit pendengar pada penyeimbang beban ini agar sesuai dengan port grup target, atau kembali ke langkah sebelumnya dan mengubah port untuk grup target.

Jika Anda belum siap untuk mendaftarkan Application Load Balancer sebagai target, pilih Register nanti dan daftarkan target nanti. Untuk informasi selengkapnya, lihat the section called “Daftarkan target”.

12. PilihBuat grup target.

AWS CLI

Untuk membuat kelompok target dari tipe alb

Gunakan perintah create-target-group. Protokol harus TCP dan port harus cocok dengan port listener Application Load Balancer.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type alb \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

CloudFormation

Untuk membuat kelompok target dari tipe alb

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::TargetGroup. Protokol harus TCP dan port harus cocok dengan port listener Application Load Balancer.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: alb
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
```

```
        - Id: !Ref myApplicationLoadBalancer
          Port: 80
```

Langkah 2: Buat Network Load Balancer dan konfigurasikan routing

Saat Anda membuat Network Load Balancer, Anda dapat mengonfigurasi tindakan default untuk meneruskan lalu lintas ke Application Load Balancer.

Console

Untuk membuat Network Load Balancer

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
   a. Untuk nama Load balancer, masukkan nama untuk Network Load Balancer Anda.
   b. Untuk Skema, pilih Mengakses Internet atau Internal. Network Load Balancer yang menghadap ke internet merutekan permintaan dari klien ke target melalui internet. Network Load Balancer internal merutekan permintaan ke target menggunakan alamat IP pribadi.
   c. Untuk jenis alamat IP Load balancer, pilih IPv4apakah klien Anda menggunakan IPv4 alamat untuk berkomunikasi dengan Network Load Balancer atau Dualstack jika klien Anda menggunakan IPv4 keduanya IPv6 dan alamat untuk berkomunikasi dengan Network Load Balancer.
6. Pemetaan jaringan
   a. Untuk VPC, pilih VPC yang sama dengan yang Anda gunakan untuk Application Load Balancer Anda. Dengan penyeimbang beban yang menghadap ke internet, hanya VPCs dengan gateway internet yang tersedia untuk dipilih.
   b. Untuk Availability Zones dan subnet, pilih setidaknya satu Availability Zones, dan pilih satu subnet per zona. Kami menyarankan Anda memilih Availability Zone yang sama yang diaktifkan untuk Application Load Balancer Anda. Ini mengoptimalkan ketersediaan, penskalaan, dan kinerja.

(Opsional) Untuk menggunakan alamat IP statis, pilih Gunakan alamat IP Elastis dalam IPv4pengaturan 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. Grup keamanan

Kami memilih grup keamanan default untuk VPC penyeimbang beban. Anda dapat memilih grup keamanan tambahan sesuai kebutuhan. Jika Anda tidak memiliki grup keamanan yang memenuhi kebutuhan Anda, pilih buat grup keamanan baru untuk membuatnya sekarang. Untuk informasi selengkapnya, lihat Membuat grup keamanan di Panduan Pengguna Amazon VPC.

> **Warning**
>
> Jika Anda tidak mengaitkan grup keamanan apa pun dengan Network Load Balancer sekarang, Anda tidak dapat mengaitkannya nanti.

> **Warning**
>
> Untuk menggunakan pendengar QUIC atau TCP_QUIC, Network Load Balancer Anda harus tidak memiliki grup keamanan.

8. 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 yang Anda buat di langkah sebelumnya.

   c. (Opsional) Pilih Tambahkan tag pendengar dan masukkan kunci tag dan nilai tag.

9. Tag penyeimbang beban

(Opsional) Perluas tag penyeimbang beban. Pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag. Untuk informasi selengkapnya, lihat Tag.

10. Ringkasan

    Tinjau konfigurasi Anda dan pilih Buat penyeimbang beban.

AWS CLI

Untuk membuat Network Load Balancer

Gunakan perintah create-load-balancer. Kami menyarankan Anda menggunakan Availability Zone yang sama yang diaktifkan untuk Application Load Balancer Anda.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Untuk menambahkan pendengar TCP

Gunakan perintah create-listener untuk menambahkan pendengar TCP. Hanya pendengar TCP yang dapat meneruskan lalu lintas ke Application Load Balancer. Untuk tindakan default, gunakan grup target yang Anda buat di langkah sebelumnya.

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

CloudFormation

Untuk membuat Network Load Balancer

Tentukan sumber daya tipe AWS::ElasticLoadBalancingV2::LoadBalancerdan sumber daya tipe AWS::ElasticLoadBalancingV2::Listener. Hanya pendengar TCP yang dapat meneruskan lalu lintas ke Application Load Balancer. Untuk tindakan default, gunakan grup target yang Anda buat di langkah sebelumnya.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-load-balancer
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup

  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Langkah 3: (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.

Menandai grup target untuk Network Load Balancer

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.

Console

Untuk mengelola tag untuk grup target

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. Pilih Simpan perubahan.

AWS CLI

Untuk menambahkan tag

Gunakan perintah add-tag. Contoh berikut menambahkan dua tag.

```
aws elbv2 add-tags \
    --resource-arns target-group-arn \
    --tags "Key=project,value=lima" "Key=department,Value=digital-media"
```

Untuk menghapus tag

Gunakan perintah remove-tag. Contoh berikut menghapus tag dengan kunci yang ditentukan.

```
aws elbv2 remove-tags \
    --resource-arns target-group-arn \
    --tag-keys project department
```

CloudFormation

Untuk menambahkan tag

Perbarui AWS::ElasticLoadBalancingV2::TargetGroupsumber daya untuk menyertakan `Tags` properti.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Menghapus grup target untuk Network Load Balancer

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.

Console

Untuk menghapus grup target

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. Pilih Hapus.

AWS CLI

Untuk menghapus grup target

Gunakan perintah delete-target-group.

```
aws elbv2 delete-target-group \
    --target-group-arn target-group-arn
```

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 instance tidak mengizinkan koneksi dari klien tetapi jaringan ACLs untuk subnet penyeimbang beban mengizinkannya, log untuk antarmuka jaringan untuk penyeimbang beban menunjukkan “TERIMA OK” untuk koneksi frontend dan backend, sedangkan log untuk antarmuka jaringan untuk instance menunjukkan “TOLAK OK” untuk koneksi.

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.

Monitor CloudWatch Internet Amazon

Anda dapat menggunakan Internet Monitor untuk visibilitas tentang bagaimana masalah internet memengaruhi kinerja dan ketersediaan antara aplikasi yang di-host AWS dan pengguna akhir Anda. Anda juga dapat menjelajahi, dalam waktu dekat, cara meningkatkan latensi yang diproyeksikan aplikasi Anda dengan beralih menggunakan layanan lain, atau dengan mengalihkan lalu lintas ke beban kerja Anda melalui yang berbeda. Wilayah AWS Untuk informasi selengkapnya, lihat Menggunakan Amazon CloudWatch Internet Monitor.

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 Elastic Load Balancing menggunakan. 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` • `TargetGroup`

Metrik	Deskripsi
`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`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`
`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` • `TargetGroup`

Metrik	Deskripsi
`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` • `TargetGroup`
`ActiveZonalShiftHostCount`	Jumlah target yang aktif berpartisipasi dalam pergeseran zona saat ini. Kriteria pelaporan: Dilaporkan saat penyeimbang beban memilih untuk pergeseran zona. Statistik: Statistik yang paling berguna adalah`Maximum`, dan`Minimum`. Dimensi • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`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`

Metrik	Deskripsi
`ConsumedLCUs`	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda. Anda membayar untuk jumlah LCUs yang Anda gunakan 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 LCUs 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_TLS`	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda untuk TLS. Anda membayar untuk jumlah LCUs 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_UDP	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda untuk UDP. Anda membayar untuk jumlah LCUs 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 ada target terdaftar. Statistik: Statistik yang paling berguna adalah Maximum dan Minimum. Dimensi • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
NewFlowCount	Jumlah total arus baru (atau koneksi) didirikan dari klien ke target dalam periode waktu. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah Sum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup

Metrik	Deskripsi
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 • TargetGroup
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 • TargetGroup

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 • TargetGroup
NewFlowCount_QUIC	Jumlah total datagram UDP yang membutuhkan keputusan routing dalam periode waktu tersebut. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah Sum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer
PeakBytesPerSecond	Byte rata-rata tertinggi yang diproses per detik, dihitung setiap 10 detik selama jendela pengambilan sampel. Metrik ini tidak termasuk lalu lintas pemeriksaan kesehatan. Reporting criteria: Selalu dilaporkan Statistics: Statistik yang paling berguna adalah Maximum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Deskripsi
PeakPacketsPerSecond	Kecepatan paket tertinggi (paket diproses sesaat), dikira setiap 10 detik saat selama window sampeling. Metrik ini mencakup lalu lintas pemeriksaan kondisi. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah Maximum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer
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: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah Sum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Deskripsi
`ProcessedBytes`	Jumlah total byte yang diproses oleh penyeimbang beban, termasuk TCP/IP header. 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`
`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`

Metrik	Deskripsi
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
ProcessedBytes_QUIC	Jumlah total byte yang diproses oleh pendengar QUIC. Reporting criteria: Ada nilai bukan nol Statistics: Statistik yang paling berguna adalah Sum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedPackets	Jumlah paket yang diproses oleh penyeimbang beban. Jumlah ini mencakup lalu lintas ke dan dari target, termasuk lalu lintas pemeriksaan kondisi. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah Sum. Dimensi • LoadBalancer • AvailabilityZone , LoadBalancer

Metrik	Deskripsi
`RejectedFlowCount`	Jumlah total arus (atau koneksi) ditolak oleh penyeimbang beban. Kriteria pelaporan: Selalu dilaporkan. Statistics: Statistik yang paling berguna adalah `Average`, `Maximum`, dan `Minimum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedFlowCount_TCP`	Jumlah aliran TCP (atau koneksi) ditolak oleh penyeimbang beban. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah `Sum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ReservedLCUs`	Jumlah unit kapasitas load balancer (LCUs) yang disediakan untuk load balancer Anda menggunakan Reservasi LCU. Reporting criteria: Ada nilai bukan nol Statistics: Semua Dimensi • `LoadBalancer`

Metrik	Deskripsi
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
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

Metrik	Deskripsi
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
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

Metrik	Deskripsi
`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`
`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`

Metrik	Deskripsi
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 ada target terdaftar. Statistik: Statistik yang paling berguna adalah Maximum dan Minimum. Dimensi • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
UnhealthyRoutingFlowCount	Jumlah aliran (atau koneksi) yang dirutekan menggunakan tindakan failover routing (gagal terbuka). Metrik ini tidak didukung untuk pendengar TLS. Kriteria pelaporan: Ada nilai bukan nol. Statistik: Statistik yang paling berguna adalah Sum.

Metrik	Deskripsi
`ZonalHealthStatus`	Jumlah Availability Zone yang dianggap sehat oleh penyeimbang beban. Penyeimbang beban memancarkan 1 untuk setiap Availability Zone yang sehat dan 0 untuk setiap Availability Zone yang tidak sehat. Kriteria pelaporan: Dilaporkan jika pemeriksaan kondisi diaktifkan. Statistik: Statistik yang paling berguna adalah `Maximum` dan `Minimum`. Dimensi • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`QUIC_Unknown_Server_ID_Packet_Drop_Count`	Jumlah datagram UDP yang dijatuhkan yang berisi ID server yang tidak terkait dengan target di Network Load Balancer. Kriteria pelaporan: Dilaporkan hanya untuk pendengar QUIC. Statistics: 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.

Dimensi	Deskripsi
`LoadBalancer`	Memfilter data metrik berdasarkan penyeimbang beban. Tentukan penyeimbang beban sebagai berikut: load-balancer-namenet/ 1234567890123456 (bagian akhir dari load balancer ARN).
`TargetGroup`	Memfilter data metrik berdasarkan grup target. Tentukan kelompok target sebagai berikut: targetgroup/ target-group-name/1234567890123456 (bagian akhir dari kelompok target ARN).

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. Saat Anda meminta statistik, aliran data yang dikembalikan diidentifikasi oleh nama metrik dan dimensi. Dimensi adalah name/value pasangan yang secara unik mengidentifikasi 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. Pada panel navigasi, silakan 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 get-metric-statisticsperintah berikut dapatkan statistik untuk metrik dan dimensi yang ditentukan. Perhatikan bahwa CloudWatch memperlakukan setiap kombinasi dimensi yang unik sebagai metrik terpisah. Anda tidak dapat mengambil statistik menggunakan kombinasi dimensi yang diterbitkan secara khusus. Anda harus menentukan dimensi yang sama yang digunakan saat metrik dibuat.

```
aws cloudwatch get-metric-statistics --namespace AWS/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**
>
> Meskipun log akses “lama” tradisional (dijelaskan di bagian ini) tetap tersedia, Network Load Balancer sekarang menawarkan opsi CloudWatch pencatatan yang disempurnakan melalui Log. CloudWatch Log menyediakan opsi pengiriman yang lebih fleksibel, termasuk ke Amazon CloudWatch Logs, Amazon Data Firehose, dan Amazon Simple Storage Service. Untuk mengonfigurasi opsi pencatatan yang ditingkatkan ini, kunjungi tab Integrasi penyeimbang beban Anda. Untuk informasi lebih lanjut tentang CloudWatch Log, lihatCloudWatch log untuk Network Load Balancer.

> **Important**
>
> Log akses dibuat hanya jika penyeimbang beban memiliki pendengar TLS, dan log hanya berisi informasi tentang permintaan TLS. Akses log merekam permintaan dengan upaya terbaik. Sebaiknya gunakan log akses untuk memahami sifat permintaan, bukan sebagai penghitungan lengkap semua permintaan.

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.

Daftar Isi

Berkas log akses

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-account-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.
client_port	Alamat IP dan port klien.
destinasi_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 `connection_time` bidang. Jika tidak ada jabat tangan TLS atau kegagalan jabat tangan TLS, nilai ini diatur ke. `-`
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 pesan halo klien 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 selesai, 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 selesai, nilai ini diatur ke. `-`

Bidang	Deskripsi
tls_keyexchange	Pertukaran kunci yang digunakan selama jabat tangan untuk TLS atau PQ-TLS. Jika negosiasi TLS atau PQ-TLS tidak selesai, nilai ini diatur ke. -
domain_name	Nilai ekstensi server_name di klien pesan hello. Nilai ini adalah URL-encoded. Jika tidak ada pesan halo klien yang valid dikirim atau ekstensi tidak ada, 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 yang dikonfigurasi di listener TLS, protokol yang cocok tidak ditemukan, atau tidak ada daftar protokol yang valid yang dikirim, nilai ini disetel 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 yang dikonfigurasi di listener TLS, protokol yang cocok tidak ditemukan, atau tidak ada daftar protokol yang valid yang dikirim, nilai ini disetel 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 tidak ada kebijakan ALPN yang dikonfigurasi di listener TLS, tidak ada pesan halo klien yang valid yang dikirim, atau ekstensi tidak ada, nilai ini disetel 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
```

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

Aktifkan log akses untuk Network Load Balancer

saat mengaktifkan pengelogan akses untuk penyeimbang beban, Anda harus menentukan nama bucket S3 tempat penyeimbang beban akan menyimpan log. Bucket harus memiliki kebijakan bucket yang memberikan izin Elastic Load Balancing untuk menulis ke bucket.

> **Important**
>
> Log akses dibuat hanya jika penyeimbang beban memiliki pendengar TLS, dan log hanya berisi informasi tentang permintaan TLS.

Persyaratan bucket

Anda dapat menggunakan bucket yang sudah ada, atau membuat bucket khusus untuk log akses. Bucket harus memenuhi persyaratan berikut.

Persyaratan

- Bucket harus ditempatkan di Wilayah yang sama dengan penyeimbang beban. Bucket dan load balancer dapat dimiliki oleh akun yang berbeda.
- 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.

Contoh kebijakan bucket

Berikut ini adalah contoh kebijakan . Untuk `Resource` elemen, ganti *`amzn-s3-demo-destination-bucket`* dengan nama bucket S3 untuk log akses Anda. Pastikan untuk menghilangkan *`Prefix/`* jika Anda tidak menggunakan awalan ember. Untuk`aws:SourceAccount`, tentukan ID AWS akun dengan penyeimbang beban. Untuk`aws:SourceArn`, ganti *`region`* dan *`012345678912`* dengan Wilayah dan ID akun penyeimbang beban, masing-masing.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-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:::amzn-s3-demo-destination-
bucket/Prefix/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:*"
                    ]
```

```
                }
            }
        }
    ]
}
```

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 .

JSON

```
{
  "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": "*"
    }
  ]
}
```

Konfigurasikan log akses

Gunakan prosedur berikut untuk mengonfigurasi log akses untuk menangkap informasi permintaan dan mengirimkan file log ke bucket S3 Anda.

Console

Untuk mengaktifkan log akses

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, aktifkan Access logs.
6. Untuk URI S3, masukkan URI S3 untuk file log Anda. URI yang Anda tentukan bergantung pada apakah Anda menggunakan awalan.
   - URI dengan awalan: s3:///*amzn-s3-demo-logging-bucketlogging-prefix*
   - URI tanpa awalan: s3://*amzn-s3-demo-logging-bucket*
7. Pilih Simpan perubahan.

AWS CLI

Untuk mengaktifkan log akses

Gunakan modify-load-balancer-attributesperintah dengan atribut terkait.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes \
        Key=access_logs.s3.enabled,Value=true \
        Key=access_logs.s3.bucket,Value=amzn-s3-demo-logging-bucket \
```

```
        Key=access_logs.s3.prefix,Value=logging-prefix
```

CloudFormation

Untuk mengaktifkan log akses

Perbarui AWS::ElasticLoadBalancingV2::LoadBalancersumber daya untuk menyertakan atribut terkait.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "access_logs.s3.enabled"
          Value: "true"
        - Key: "access_logs.s3.bucket"
          Value: "amzn-s3-demo-logging-bucket"
        - Key: "access_logs.s3.prefix"
          Value: "logging-prefix"
```

Nonaktifkan log akses untuk Network Load Balancer

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 Membuat, mengonfigurasi, dan bekerja dengan bucket S3 di Panduan Pengguna Amazon S3.

Console

Untuk menonaktifkan log akses

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.

AWS CLI

Untuk menonaktifkan log akses

Gunakan perintah modify-load-balancer-attributes.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes Key=access_logs.s3.enabled,Value=false
```

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 Penyeimbang Beban Jaringan.

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. Selain itu, grup keamanan untuk Load Balancer Anda harus mengizinkan lalu lintas ke instance. Untuk informasi selengkapnya, lihat Memperbarui grup keamanan untuk Network Load Balancer.

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 Jaringan ACLs.

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. Selain itu, grup keamanan untuk Load Balancer Anda harus mengizinkan lalu lintas ke instance. Untuk informasi selengkapnya, lihat Memperbarui grup keamanan untuk Network Load Balancer.

Daftar kontrol akses jaringan (ACL) tidak memungkinkan lalu lintas

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

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.

ID server yang dikonfigurasi tidak cocok dengan ID yang dikonfigurasi pada target

Jika Anda menggunakan pendengar QUIC, pastikan ID yang dikonfigurasi pada target cocok dengan ID yang dikonfigurasi dengan grup target Network Load Balancer.

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 sebuah instance adalah klien dari penyeimbang beban yang terdaftar dengannya dan memiliki pelestarian IP klien yang diaktifkan, koneksi hanya berhasil jika permintaan dirutekan ke instance yang berbeda. Jika permintaan dirutekan ke instance yang sama dengan yang dikirim, waktu koneksi habis karena alamat IP sumber dan tujuan adalah sama. Perhatikan bahwa ini berlaku untuk pod Amazon EKS yang berjalan di instance node pekerja EC2 yang sama, meskipun mereka memiliki alamat IP yang berbeda.

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

- Nonaktifkan pelestarian IP klien. Sebagai gantinya, gunakan Proxy Protocol v2 untuk mendapatkan alamat IP klien.
- Pastikan bahwa kontainer yang harus berkomunikasi berada pada instance 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 untuk aliran backend

Dengan PrivateLink lalu lintas atau 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 batas ini, ada kemungkinan peningkatan kesalahan alokasi port. Anda dapat melacak kesalahan alokasi port menggunakan `PortAllocationErrorCount` metrik. Anda dapat melacak koneksi aktif menggunakan `ActiveFlowCount` metrik. Untuk informasi selengkapnya, lihat CloudWatch metrik untuk Network Load Balancer.

Untuk memperbaiki kesalahan alokasi port, kami sarankan Anda menambahkan target ke grup target.

Atau, jika Anda tidak dapat menambahkan target ke grup target, Anda dapat menambahkan hingga 7 alamat IP sekunder ke antarmuka jaringan penyeimbang beban. Alamat IP sekunder secara otomatis dialokasikan dari blok IPv4 CIDR dari subnet yang sesuai. Setiap alamat IP sekunder mengkonsumsi 6 unit pengalamatan jaringan. Perhatikan bahwa setelah Anda menambahkan alamat IP sekunder, Anda tidak dapat menghapusnya. Satu-satunya cara untuk melepaskan alamat IP sekunder adalah dengan menghapus penyeimbang beban.

Kegagalan pembentukan koneksi TCP intermiten atau penundaan pembentukan koneksi TCP

Ketika pelestarian alamat IP klien diaktifkan, klien dapat terhubung ke alamat IP tujuan yang berbeda menggunakan port fana sumber yang sama. Alamat IP tujuan ini dapat berasal dari penyeimbang beban yang sama (di Availability Zone yang berbeda) ketika penyeimbangan beban lintas zona diaktifkan atau Network Load Balancer berbeda yang menggunakan alamat IP target yang sama dan port terdaftar. Dalam hal ini, jika koneksi ini diarahkan ke alamat IP target dan port yang sama, target akan melihat koneksi duplikat, karena mereka berasal dari alamat IP klien dan port yang sama. Hal ini menyebabkan kesalahan koneksi dan penundaan saat membuat salah satu koneksi ini. Ini

sering terjadi ketika perangkat NAT di depan klien, dan alamat IP sumber dan port sumber yang sama dialokasikan saat menghubungkan ke beberapa alamat IP Network Load Balancer secara bersamaan.

Anda dapat mengurangi jenis kesalahan koneksi ini dengan meningkatkan jumlah port fana sumber yang dialokasikan oleh klien atau perangkat NAT, atau dengan meningkatkan jumlah target untuk penyeimbang beban. Kami menyarankan klien mengubah port sumber yang digunakan saat menghubungkan kembali setelah kegagalan koneksi ini. Untuk mencegah jenis kesalahan koneksi ini, jika Anda menggunakan Network Load Balancer tunggal, Anda dapat mempertimbangkan untuk menonaktifkan penyeimbangan beban lintas zona, atau jika menggunakan beberapa Network Load Balancer, Anda dapat mempertimbangkan untuk tidak menggunakan alamat IP target yang sama dan port yang terdaftar di beberapa kelompok target. Atau, Anda dapat mempertimbangkan untuk menonaktifkan pelestarian IP klien. Jika Anda membutuhkan IP klien, Anda dapat menggunakan mengambilnya menggunakan Proxy Protocol v2. Untuk mempelajari lebih lanjut tentang Proxy Protocol v2, lihatProtokol proxy.

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.

Lalu lintas didistribusikan secara tidak merata antar target

Pendengar TCP dan TLS merutekan koneksi TCP dan pendengar UDP merutekan aliran UDP. Load balancer memilih target menggunakan algoritma flow hash. Koneksi tunggal dari klien secara inheren lengket.

Jika Anda melihat bahwa beberapa target tampaknya menerima lebih banyak lalu lintas daripada yang lain, kami sarankan Anda meninjau log aliran VPC. Bandingkan jumlah koneksi unik untuk setiap alamat IP target. Jaga agar jendela waktu sesingkat mungkin, karena pendaftaran target, deregistrasi, dan target yang tidak sehat memengaruhi nomor koneksi ini.

Berikut ini adalah skenario yang memungkinkan di mana koneksi dapat didistribusikan secara tidak merata:

- Jika Anda memulai dengan sejumlah kecil target dan kemudian mendaftarkan target tambahan nanti, target asli masih memiliki koneksi dengan klien. Dengan beban kerja HTTP, keepalives memastikan bahwa klien menggunakan kembali koneksi. Jika Anda menurunkan keepalives maksimal pada aplikasi web Anda, klien akan membuka koneksi baru lebih sering.
- Jika kelengketan kelompok target diaktifkan, ada sejumlah kecil klien, dan klien berkomunikasi melalui perangkat NAT dengan alamat IP sumber tunggal, koneksi dari klien ini diarahkan ke target yang sama.
- Jika penyeimbangan beban lintas zona dinonaktifkan dan klien lebih memilih alamat IP penyeimbang beban dari salah satu zona penyeimbang beban, koneksi akan didistribusikan secara tidak merata di antara zona penyeimbang beban.

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 yang diaktifkan AZs dalam hasilnya.

Paket IP yang terfragmentasi tidak dirutekan ke target

Network Load Balancer tidak mendukung paket IP yang terfragmentasi untuk lalu lintas non-UDP.

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 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 salah satu pendengar Anda memiliki:
    >
    > - Kebijakan TLS pasca-kuantum FIPS - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09`
    > - Kebijakan FIPS - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`
    > - Kebijakan TLS pasca-kuantum - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-PQ-2025-09`
    > - Kebijakan TLS 1.3 - Koneksi backend digunakan `ELBSecurityPolicy-TLS13-1-0-2021-06`
    > - Semua kebijakan TLS lainnya yang digunakan koneksi backend `ELBSecurityPolicy-2016-08`
    >
    > 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

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

Untuk 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 penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas. Jika kuota belum tersedia di Service Quotas, ajukan permintaan kenaikan kuota layanan.

Kuota

- Load balancer
- Kelompok-kelompok target
- Unit Kapasitas Load Balancer

Load balancer

Anda Akun AWS memiliki kuota berikut yang terkait dengan Network Load Balancers.

Nama	Default	Dapat disesuaikan
Sertifikat per Penyeimbang Beban Jaringan	25	Ya
Listener per Penyeimbang Beban Jaringan	50	Tidak
Network Load Balancer ENIs untuk VPC	1,200	Ya
Penyeimbang Beban Jaringan per Wilayah	50	Ya
Subnet per Availability Zone per Penyeimbang Beban Jaringan	500 [2, 3]	Ya
Target per Penyeimbang Beban Jaringan	3.000 [3]	Ya

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

[2] Jika target terdaftar dengan N kelompok target, itu dihitung sebagai target N menuju batas ini. Setiap Application Load Balancer yang menjadi 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 penyeimbangan beban lintas zona diaktifkan, maksimum adalah 500 target per penyeimbang beban, terlepas dari jumlah Availability Zone.

Kelompok-kelompok target

Kuota berikut adalah untuk kelompok sasaran.

Nama	Default	Dapat disesuaikan
Grup Target per Wilayah	3.000 +	Ya
Target per Grup Target per Wilayah (contoh atau alamat IP)	1.000	Ya
Target per Grup Target per Wilayah (Application Load Balancers)	1	Tidak

[1] Kuota ini dibagi oleh Application Load Balancers dan Network Load Balancer.

Unit Kapasitas Load Balancer

Kuota berikut adalah untuk Load Balancer Capacity Units LCUs ().

Nama	Default	Dapat disesuaikan
Unit Kapasitas Load Balancer Jaringan Cadangan (LCUs) per Network Load Balancer, per zona ketersediaan	45000	Ya

Nama	Default	Dapat disesuaikan
Unit Kapasitas Load Balancer Jaringan Cadangan (LCU) per Wilayah	0	Ya

Riwayat dokumen untuk Penyeimbang Beban

Tabel berikut menjelaskan rilis untuk Penyeimbang Beban Jaringan.

Perubahan	Deskripsi	Tanggal
Kelompok sasaran tertimbang	Rilis ini menambahkan dukungan untuk tindakan default dengan grup target tertimbang.	November 19, 2025
Dukungan Protokol QUIC dan TCP_QUIC	Rilis ini menambahkan dukungan untuk protokol QUIC dan TCP_QUIC.	November 13, 2025
IPv4 Alamat sekunder	Rilis ini menambahkan dukungan untuk menambahk an IPv4 alamat sekunder ke antarmuka jaringan penyeimba ng beban.	Juli 29, 2025
Nonaktifkan Availability Zone	Rilis ini menambahkan dukungan untuk menonakti fkan Availability Zone untuk penyeimbang beban yang ada.	Februari 13, 2025
Reservasi Unit Kapasitas	Rilis ini menambahkan dukungan untuk menetapkan kapasitas minimum penyeimba ng beban Anda.	November 20, 2024
Dukungan UDP IPv6 untuk penyeimbang beban dualstack	Rilis ini memungkinkan klien untuk mengakses aplikasi berbasis UDP menggunakan. IPv6	Oktober 31, 2024
Sertifikat RSA 3072-bit dan ECDSA 256/384/521-bit	Rilis ini menambahkan dukungan untuk sertifikat	Januari 19, 2024

	RSA 3072-bit, dan sertifikat Elliptic Curve Digital Signature Algorithm (ECDSA) 256, 384 dan 521-bit via (ACM). AWS Certificate Manager	
Pengakhiran FIPS 140-3 TLS	Rilis ini menambahkan kebijakan keamanan yang menggunakan modul kripotografi FIPS 140-3 saat mengakhiri 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 mempertahankan koneksi aktif ke target yang gagal pemeriksaan kesehatan.	12 Oktober 2023
Pengakhiran koneksi UDP default	Rilis ini menambahkan dukungan untuk mengakhiri koneksi UDP di akhir batas waktu deregistrasi secara default.	12 Oktober 2023
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
IPv6 kelompok sasaran	Rilis ini menambahkan dukungan untuk mengkonfigurasi grup IPv6 target untuk Network Load Balancers.	23 November 2021
IPv6 penyeimbang beban internal	Rilis ini menambahkan dukungan untuk mengkonfigurasi grup IPv6 target 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 IPv4 alamat 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 rentang IPv4 alamat 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 memungkinkan 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 Penyeimbang 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.