



AWS PrivateLink

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: AWS PrivateLink

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS PrivateLink?	1
Kasus penggunaan	1
Bekerja dengan titik akhir VPC	3
Harga	3
Konsep	4
Diagram arsitektur	4
Penyedia	5
Konsumen layanan atau sumber daya	6
AWS PrivateLink koneksi	9
Zona yang di-hosting privat	9
Memulai	11
Langkah 1: Buat VPC dengan subnet	12
Langkah 2: Luncurkan instance	12
Langkah 3: Uji CloudWatch akses	14
Langkah 4: Buat titik akhir VPC untuk mengakses CloudWatch	15
Langkah 5: Uji titik akhir VPC	15
Langkah 6: Bersihkan	16
Akses Layanan AWS	17
Gambaran umum	18
Nama host DNS	19
Resolusi DNS	21
DNS privat	21
Subnet dan Zona Ketersediaan	22
Jenis alamat IP	25
Jenis IP catatan DNS	26
Layanan yang terintegrasi	27
Lihat tersedia Layanan AWS nama	52
Melihat informasi tentang layanan	53
Lihat dukungan kebijakan titik akhir	54
Lihat dukungan IPv6	56
Cross-region diaktifkan Layanan AWS	57
Lihat tersedia Layanan AWS nama	52
Izin dan Pertimbangan	58
Membuat titik akhir antarmuka ke Layanan AWS di daerah lain	59

Membuat sebuah titik akhir antarmuka	60
Prasyarat	60
Buat VPC endpoint	61
Subnet bersama	62
ICMP	63
Konfigurasi titik akhir antarmuka	63
Menambah atau menghapus subnet	63
Grup keamanan asosiasi	64
Edit kebijakan titik akhir VPC	65
Aktifkan nama DNS pribadi	65
Kelola tanda	66
Menerima peringatan untuk peristiwa titik akhir antarmuka	67
Buat notifikasi SNS	67
Menambahkan kebijakan akses	68
Menambahkan kebijakan utama	69
Menghapus titik akhir antarmuka	70
Titik akhir Gateway	70
Gambaran umum	71
Perutean	72
Keamanan	73
Jenis alamat IP	74
Jenis IP catatan DNS	74
Titik akhir untuk Amazon S3	76
Titik akhir untuk DynamoDB	88
Akses produk SaaS	96
Gambaran umum	96
Membuat sebuah titik akhir antarmuka	97
Bagikan layanan Anda	99
Gambaran umum	99
Nama host DNS	100
DNS privat	101
Subnet dan Zona Ketersediaan	101
Cross-Region akses	102
Jenis alamat IP	103
Membuat layanan titik akhir	104
Pertimbangan-pertimbangan	105

Prasyarat	106
Membuat layanan titik akhir	106
Jadikan layanan endpoint Anda tersedia untuk konsumen layanan	108
Menghubungkan ke layanan titik akhir sebagai konsumen layanan	108
Mengkonfigurasi layanan titik akhir	109
Kelola izin	110
Menerima atau tolak permintaan koneksi	111
Kelola penyeimbang beban	113
Menggaitkan nama DNS pribadi	114
Ubah Wilayah yang didukung	115
Ubah jenis alamat IP yang didukung	116
Kelola tanda	117
Kelola nama DNS	118
Verifikasi kepemilikan domain	119
Dapatkan nama dan nilainya	119
Menambahkan catatan TXT ke server DNS domain Anda	120
Periksa apakah catatan TXT diterbitkan	122
Memecahkan masalah verifikasi domain	123
Menerima peringatan untuk acara layanan titik akhir	123
Buat notifikasi SNS	124
Menambahkan kebijakan akses	125
Menambahkan kebijakan utama	125
Menghapus layanan titik akhir	126
Akses peralatan virtual	128
Gambaran umum	128
Jenis alamat IP	130
Perutean	131
Membuat layanan titik akhir Gateway Load Balancer	132
Pertimbangan-pertimbangan	132
Prasyarat	133
Buat layanan endpoint	133
Jadikan layanan titik akhir Anda tersedia	134
Membuat titik akhir Gateway Load Balancer	135
Pertimbangan-pertimbangan	135
Prasyarat	136
Buat titik akhir	136

Konfigurasikan perutean	137
Kelola tanda	139
Hapus titik akhir	139
Akses sumber daya VPC	141
Gambaran umum	141
Pertimbangan-pertimbangan	142
Nama host DNS	142
Resolusi DNS	144
DNS privat	144
Subnet dan Zona Ketersediaan	144
Jenis alamat IP	145
Membuat titik akhir sumber daya	145
Prasyarat	145
Membuat titik akhir sumber daya VPC	146
Kelola titik akhir sumber daya	147
Hapus titik akhir	147
Memperbarui titik akhir	148
Akses segmen jaringan	149
Gambaran umum	149
Pertimbangan-pertimbangan	150
Geneve enkapsulasi	150
Nama host DNS	150
Resolusi DNS	150
DNS privat	151
Subnet dan Zona Ketersediaan	151
Jenis alamat IP	151
Membuat titik akhir terowongan	152
Prasyarat	152
Membuat titik akhir VPC terowongan	152
Akses jaringan layanan	154
Gambaran umum	155
Nama host DNS	155
Resolusi DNS	156
DNS privat	156
Subnet dan Zona Ketersediaan	157
Jenis alamat IP	158

Membuat titik akhir jaringan layanan	158
Prasyarat	158
Membuat titik akhir jaringan layanan	159
Mengelola titik akhir jaringan layanan	160
Hapus titik akhir	160
Memperbarui titik akhir jaringan layanan	161
Konfigurasi sumber daya	162
Jenis konfigurasi sumber daya	162
Gateway sumber daya	163
Nama domain khusus untuk penyedia sumber daya	163
Nama domain khusus untuk konsumen sumber daya	164
Nama domain khusus untuk pemilik jaringan layanan	166
Definisi sumber daya	166
Protokol	167
Rentang pelabuhan	167
Mengakses sumber daya	167
Asosiasi dengan jenis jaringan layanan	168
Jenis jaringan layanan	169
Berbagi konfigurasi sumber daya melalui AWS RAM	169
Memantau	170
Buat konfigurasi sumber daya	170
Kelola asosiasi	172
Kelola asosiasi sumber daya jaringan layanan	172
Kelola asosiasi titik akhir VPC sumber daya	173
Gateway sumber daya	163
Pertimbangan-pertimbangan	175
Grup keamanan	176
Jenis alamat IP	176
Alamat IPv4 per ENI	177
Resolusi DNS Konfigurasi Sumber Daya	177
Membuat gateway sumber daya	177
Menghapus gateway sumber daya	178
Manajemen identitas dan akses	180
Audiens	180
Mengautentikasi dengan identitas	181
Akun AWS pengguna root	181

Identitas terfederasi	181
Pengguna dan grup IAM	181
Peran IAM	182
Mengelola akses menggunakan kebijakan	182
Identity-based kebijakan	182
Resource-based kebijakan	183
Jenis-jenis kebijakan lain	183
Berbagai jenis kebijakan	184
Bagaimana AWS PrivateLink bekerja dengan IAM	184
Identity-based kebijakan	185
Resource-based kebijakan	185
Tindakan kebijakan	186
Sumber daya kebijakan	186
Kunci kondisi kebijakan	187
ACL	187
ABAC	187
Kredensial sementara	188
Izin principal	188
Peran layanan	188
Peran Service-linked	189
Identity-based contoh kebijakan	189
Kontrol penggunaan titik akhir VPC	189
Kontrol pembuatan titik akhir VPC berdasarkan pemilik layanan	190
Kontrol nama DNS pribadi yang dapat ditentukan untuk layanan titik akhir VPC	191
Kontrol nama layanan yang dapat ditentukan untuk layanan titik akhir VPC	192
Kebijakan titik akhir	193
Pertimbangan-pertimbangan	193
Kebijakan titik akhir default	194
Kebijakan untuk titik akhir antarmuka	194
Prinsip untuk titik akhir gateway	194
Memperbarui kebijakan titik akhir VPC	195
AWS kebijakan terkelola	196
Pembaruan kebijakan	196
CloudWatch metrik	197
Metrik dan dimensi titik akhir	197
Metrik dan dimensi layanan titik akhir	200

Lihat CloudWatch metrik	203
Gunakan aturan Wawasan Kontributor bawaan	204
Aktifkan aturan Contributor Insights	205
Nonaktifkan aturan Wawasan Kontributor	206
Hapus aturan Wawasan Kontributor	207
Kuota	208
Riwayat dokumen	210
.....	ccxiv

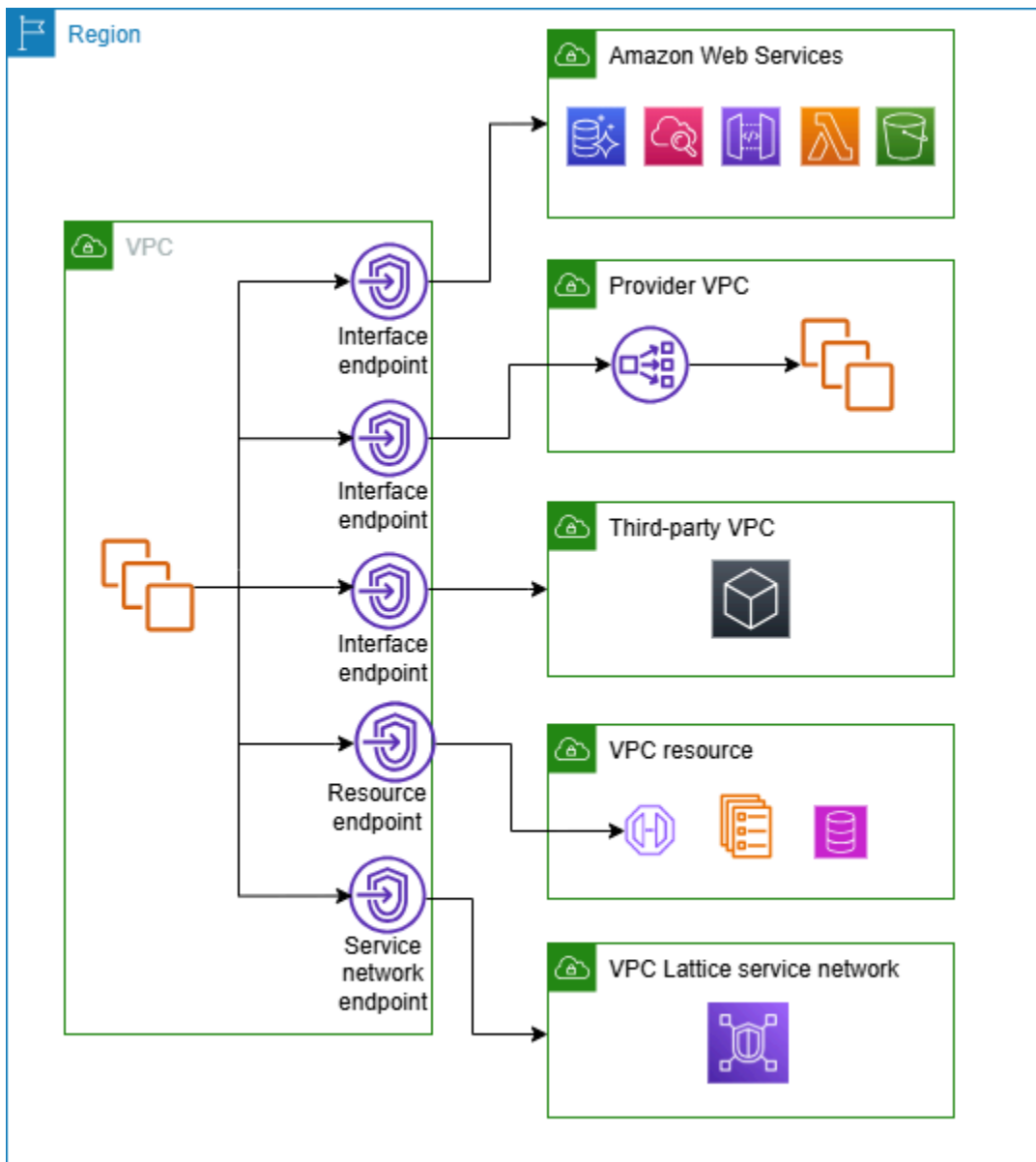
Apa itu AWS PrivateLink?

AWS PrivateLink adalah teknologi yang sangat tersedia dan dapat diskalakan yang dapat Anda gunakan untuk menghubungkan VPC Anda secara pribadi ke layanan dan sumber daya seolah-olah mereka ada di VPC Anda. Anda tidak perlu menggunakan gateway internet, perangkat NAT, alamat IP publik, Direct Connect koneksi, atau AWS Site-to-Site VPN koneksi untuk memungkinkan komunikasi dengan layanan atau sumber daya dari subnet pribadi Anda. Oleh karena itu, Anda mengontrol titik akhir API tertentu, situs, layanan, dan sumber daya yang dapat dijangkau dari VPC Anda.

Kasus penggunaan

Anda dapat membuat titik AWS PrivateLink akhir VPC berbasis untuk mengakses layanan, sumber daya, dan segmen jaringan di seluruh batas VPC dan akun. Anda dapat membuat layanan titik akhir VPC Anda sendiri dan membuatnya tersedia untuk AWS pelanggan lain. Untuk informasi selengkapnya, lihat [the section called “Konsep”](#).

Dalam diagram berikut, VPC di sebelah kiri memiliki beberapa instans Amazon EC2 di subnet pribadi dan lima titik akhir VPC - tiga titik akhir VPC antarmuka, titik akhir VPC sumber daya, dan titik akhir VPC jaringan layanan. Titik akhir VPC antarmuka pertama terhubung ke AWS layanan. Titik akhir VPC antarmuka kedua terhubung ke layanan yang dihosting oleh AWS akun lain (layanan titik akhir VPC). Titik akhir VPC antarmuka ketiga terhubung ke layanan mitra AWS Marketplace. Titik akhir VPC sumber daya terhubung ke database. Titik akhir VPC jaringan layanan terhubung ke jaringan layanan.



Pelajari selengkapnya

- [Konsep](#)
- [Akses Layanan AWS](#)
- [Akses produk SaaS](#)
- [Akses peralatan virtual](#)
- [Bagikan layanan Anda](#)

Bekerja dengan titik akhir VPC

Anda dapat membuat, mengakses, dan mengelola titik akhir VPC menggunakan salah satu dari berikut ini:

- Konsol Manajemen AWS Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses AWS PrivateLink sumber daya Anda. Buka konsol Amazon VPC dan pilih Endpoints atau Endpoint services.
- AWS Command Line Interface (AWS CLI) - Menyediakan perintah untuk serangkaian luas Layanan AWS, termasuk AWS PrivateLink. Untuk informasi selengkapnya tentang perintah untuk AWS PrivateLink, lihat [ec2](#) di Referensi Perintah AWS CLI.
- CloudFormation- Buat template yang menggambarkan AWS sumber daya Anda. Anda menggunakan template untuk menyediakan dan mengelola sumber daya ini sebagai satu unit. Untuk informasi selengkapnya, lihat AWS PrivateLink sumber daya berikut:
 - [AWS::EC2::VPCEndpoint](#)
 - [AWS::EC2::VPCEndpointConnectionNotification](#)
 - [AWS::EC2::VPCEndpointService](#)
 - [AWS::EC2::VPCEndpointServicePermissions](#)
 - [AWS::ElasticLoadBalancingV2::LoadBalancer](#)
- AWS SDK — Menyediakan API khusus bahasa. SDK menangani banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan menangani kesalahan. Untuk informasi lebih lanjut, lihat [Alat untuk Membangun di AWS](#).
- Kueri API — Menyediakan tindakan API tingkat rendah yang Anda hubungi menggunakan permintaan HTTPS. Menggunakan Query API adalah cara paling langsung untuk mengakses Amazon VPC. Namun, aplikasi Anda harus menangani detail tingkat rendah seperti menghasilkan hash untuk menandatangani permintaan dan menangani kesalahan. Untuk informasi selengkapnya, lihat [AWS PrivateLink tindakan](#) di Referensi API Amazon EC2.

Harga

Untuk informasi tentang harga untuk titik akhir VPC, lihat [AWS PrivateLink Harga](#).

AWS PrivateLink konsep

Anda dapat menggunakan Amazon VPC untuk menentukan cloud pribadi virtual (VPC), yang merupakan jaringan virtual yang terisolasi secara logis. Anda dapat mengizinkan klien di VPC Anda untuk terhubung ke tujuan di luar VPC tersebut. Misalnya, tambahkan gateway internet ke VPC untuk mengizinkan akses ke internet, atau tambahkan koneksi VPN untuk mengizinkan akses ke jaringan lokal Anda. Atau, gunakan AWS PrivateLink untuk mengizinkan klien di VPC Anda terhubung ke layanan dan sumber daya di VPC lain menggunakan alamat IP pribadi, seolah-olah layanan dan sumber daya tersebut di-host langsung di VPC Anda.

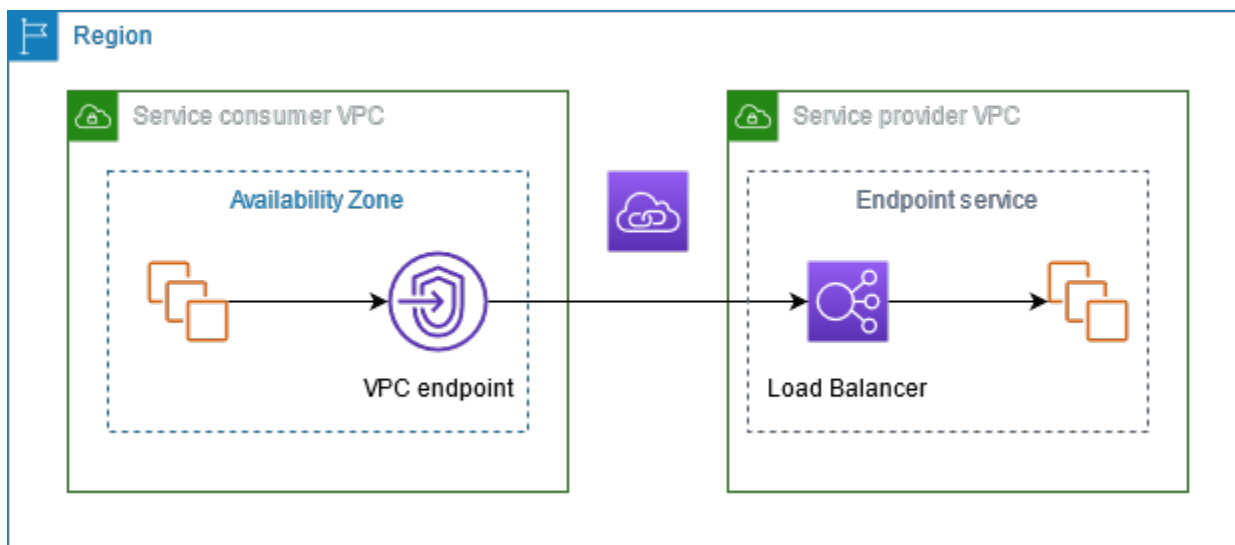
Berikut ini adalah konsep penting untuk dipahami saat Anda mulai menggunakan AWS PrivateLink.

Daftar Isi

- [Diagram arsitektur](#)
- [Penyedia](#)
- [Konsumen layanan atau sumber daya](#)
- [AWS PrivateLink koneksi](#)
- [Zona yang di-hosting privat](#)

Diagram arsitektur

Diagram berikut memberikan gambaran tingkat tinggi tentang cara kerja AWS PrivateLink janya. Konsumen membuat titik akhir VPC untuk terhubung ke layanan titik akhir dan sumber daya yang dihosting oleh penyedia.



Penyedia

Memahami konsep yang terkait dengan penyedia.

Penyedia layanan

Pemilik layanan adalah penyedia layanan. Penyedia layanan termasuk AWS, AWS Mitra, dan lainnya Akun AWS. Penyedia layanan dapat meng-host layanan mereka menggunakan AWS sumber daya, seperti instans EC2, atau menggunakan server lokal.

Penyedia sumber daya

Pemilik sumber daya, misalnya database atau instans Amazon EC2, adalah penyedia sumber daya. Penyedia sumber daya termasuk AWS layanan, AWS Mitra, dan AWS akun lainnya. Penyedia sumber daya dapat meng-host sumber daya mereka di VPC atau lokal.

Konsep

- [Layanan titik akhir](#)
- [Nama layanan](#)
- [Status layanan](#)
- [Konfigurasi sumber daya](#)
- [Gateway sumber daya](#)

Layanan titik akhir

Penyedia layanan membuat layanan titik akhir untuk membuat layanan mereka tersedia di Wilayah. Penyedia layanan harus menentukan penyeimbang beban saat membuat layanan titik akhir. Penyeimbang beban menerima permintaan dari konsumen layanan dan mengarahkannya ke layanan Anda.

Secara default, layanan titik akhir Anda tidak tersedia untuk konsumen layanan. Anda harus menambahkan izin yang memungkinkan prinsipal AWS tertentu untuk terhubung ke layanan titik akhir Anda.

Nama layanan

Setiap layanan endpoint diidentifikasi dengan nama layanan. Konsumen layanan harus menentukan nama layanan saat membuat titik akhir VPC. Konsumen layanan dapat menanyakan nama layanan

untuk Layanan AWS. Penyedia layanan harus membagikan nama layanan mereka dengan konsumen layanan.

Status layanan

Berikut ini adalah kemungkinan status untuk layanan titik akhir:

- Tertunda - Layanan titik akhir sedang dibuat.
- Tersedia - Layanan titik akhir tersedia.
- Gagal - Layanan titik akhir tidak dapat dibuat.
- Menghapus - Penyedia layanan menghapus layanan titik akhir dan penghapusan sedang berlangsung.
- Dihapus - Layanan titik akhir dihapus.

Konfigurasi sumber daya

Penyedia sumber daya membuat konfigurasi sumber daya untuk berbagi sumber daya. Konfigurasi sumber daya adalah objek logis yang mewakili sumber daya tunggal seperti database, sekelompok sumber daya, atau segmen jaringan (satu set rentang CIDR). Sumber daya dapat berupa alamat IP, target nama domain, atau database [Amazon Relational Database Service](#) (Amazon RDS).

Saat berbagi dengan akun lain, penyedia sumber daya harus berbagi sumber daya melalui [AWS Resource Access Manager](#) (AWS RAM) berbagi sumber daya untuk mengizinkan prinsi AWS pal tertentu di akun lain terhubung ke sumber daya melalui titik akhir VPC sumber daya.

Konfigurasi sumber daya dapat dikaitkan dengan jaringan layanan yang dihubungkan oleh prinsipal melalui titik akhir VPC jaringan layanan.

Gateway sumber daya

Gateway sumber daya adalah titik masuk ke VPC dari mana sumber daya dibagikan. Penyedia membuat gateway sumber daya untuk berbagi sumber daya dari VPC.

Konsumen layanan atau sumber daya

Pengguna layanan atau sumber daya adalah konsumen. Konsumen dapat mengakses layanan titik akhir dan sumber daya dari VPC mereka atau dari lokal.

Konsep

- [Titik akhir VPC](#)
- [Antarmuka jaringan titik akhir](#)
- [Kebijakan titik akhir](#)
- [Status titik akhir](#)

Titik akhir VPC

Konsumen membuat titik akhir VPC untuk menghubungkan VPC mereka ke layanan atau sumber daya titik akhir. Konsumen harus menentukan layanan titik akhir, sumber daya, atau jaringan layanan saat membuat titik akhir VPC. Ada beberapa jenis titik akhir VPC. Anda harus membuat jenis titik akhir VPC yang Anda butuhkan.

- **Interface-** Buat titik akhir antarmuka untuk mengirim lalu lintas TCP atau UDP ke layanan endpoint. Lalu lintas yang ditujukan untuk layanan titik akhir diselesaikan menggunakan DNS.
- **GatewayLoadBalancer-** Buat titik akhir Gateway Load Balancer untuk mengirim lalu lintas ke armada peralatan virtual menggunakan alamat IP pribadi. Anda merutekan lalu lintas dari VPC Anda ke titik akhir Gateway Load Balancer menggunakan tabel rute. Gateway Load Balancer mendistribusikan lalu lintas ke peralatan virtual dan dapat menskalakan sesuai permintaan.
- **Resource-** Buat titik akhir sumber daya untuk mengakses sumber daya yang dibagikan dengan Anda dan berada di VPC lain. Titik akhir sumber daya memungkinkan Anda mengakses sumber daya secara pribadi dan aman seperti database, instans Amazon EC2, titik akhir aplikasi, target nama domain, atau alamat IP yang mungkin berada di subnet pribadi di VPC lain atau di lingkungan lokal. Titik akhir sumber daya tidak memerlukan penyeimbang beban, dan memungkinkan Anda mengakses sumber daya secara langsung.
- **Tunnel-** Buat titik akhir terowongan untuk mengakses segmen jaringan yang dibagikan dengan Anda dari VPC atau akun lain. Titik akhir terowongan memungkinkan Anda melakukan terowongan secara pribadi dan aman ke segmen jaringan (daftar rentang CIDR) dan mengakses sumber daya apa pun yang terletak di segmen tersebut. Titik akhir terowongan mengharuskan Anda untuk merangkum lalu lintas aplikasi di GENEVE.
- **Service network-** Buat titik akhir jaringan layanan untuk mengakses jaringan layanan yang Anda buat atau dibagikan dengan Anda. Anda dapat menggunakan titik akhir jaringan layanan tunggal untuk mengakses beberapa sumber daya dan layanan yang terkait dengan jaringan layanan secara pribadi dan aman.

Ada jenis titik akhir VPC lain, Gateway, yang membuat titik akhir gateway untuk mengirim lalu lintas ke Amazon S3 atau DynamoDB. Titik akhir gateway tidak digunakan AWS PrivateLink, tidak seperti jenis titik akhir VPC lainnya. Untuk informasi selengkapnya, lihat [the section called “Titik akhir Gateway”](#).

Antarmuka jaringan titik akhir

Antarmuka jaringan titik akhir adalah antarmuka jaringan yang dikelola permintaan yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan ke layanan titik akhir, sumber daya, atau jaringan layanan. Untuk setiap subnet yang Anda tentukan saat membuat titik akhir VPC, kami membuat antarmuka jaringan titik akhir di subnet.

Jika titik akhir VPC mendukung IPv4, antarmuka jaringan titik puncaknya memiliki alamat IPv4. Jika titik akhir VPC mendukung IPv6, antarmuka jaringan titik puncaknya memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan titik akhir tidak dapat dijangkau dari internet. Saat Anda menjelaskan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Kebijakan titik akhir

Kebijakan titik akhir VPC adalah kebijakan sumber daya IAM yang Anda lampirkan ke titik akhir VPC. Ini menentukan prinsipal mana yang dapat menggunakan titik akhir VPC untuk mengakses layanan titik akhir. Kebijakan titik akhir VPC default mengizinkan semua tindakan oleh semua prinsipal pada semua sumber daya melalui titik akhir VPC.

Status titik akhir

Saat Anda membuat titik akhir VPC antarmuka, layanan titik akhir menerima permintaan koneksi. Penyedia layanan dapat menerima atau menolak permintaan. Jika penyedia layanan menerima permintaan, konsumen layanan dapat menggunakan titik akhir VPC setelah memasuki status Tersedia.

Berikut ini adalah kemungkinan status untuk titik akhir VPC:

- `PendingAcceptance` - Permintaan koneksi tertunda. Ini adalah keadaan awal jika permintaan diterima secara manual.
- `Tertunda` - Penyedia layanan menerima permintaan koneksi. Ini adalah keadaan awal jika permintaan diterima secara otomatis. Titik akhir VPC kembali ke status ini jika konsumen layanan memodifikasi titik akhir VPC.

- Tersedia - Titik akhir VPC tersedia untuk digunakan.
- Ditolak - Penyedia layanan menolak permintaan koneksi. Penyedia layanan juga dapat menolak koneksi setelah tersedia untuk digunakan.
- Kedaluwarsa - Permintaan koneksi kedaluwarsa.
- Gagal - Titik akhir VPC tidak dapat dibuat tersedia.
- Menghapus - Konsumen layanan menghapus titik akhir VPC dan penghapusan sedang berlangsung.
- Dihapus - Titik akhir VPC dihapus.

AWS PrivateLink API mengembalikan status yang mungkin menggunakan kotak unta.

AWS PrivateLink koneksi

Lalu lintas dari VPC Anda dikirim ke layanan atau sumber daya titik akhir menggunakan koneksi antara titik akhir VPC dan layanan atau sumber daya titik akhir. Lalu lintas antara titik akhir VPC dan layanan titik akhir atau sumber daya tetap berada di dalam AWS jaringan, tanpa melintasi internet publik.

Penyedia layanan menambahkan [izin](#) sehingga konsumen layanan dapat mengakses layanan titik akhir. Konsumen layanan memulai koneksi dan penyedia layanan menerima atau menolak permintaan koneksi. Pemilik sumber daya atau pemilik jaringan layanan berbagi konfigurasi sumber daya atau jaringan layanan dengan konsumen AWS Resource Access Manager sehingga konsumen dapat mengakses sumber daya atau jaringan layanan.

Dengan titik akhir VPC antarmuka, konsumen dapat menggunakan kebijakan [titik akhir](#) untuk mengontrol prinsipal IAM mana yang dapat menggunakan titik akhir VPC untuk mengakses layanan atau sumber daya titik akhir.

Zona yang di-hosting privat

Zona yang di hosting adalah wadah untuk catatan DNS yang menentukan cara merutekan lalu lintas untuk domain atau subdomain. Dengan zona publik yang di hosting, catatan menentukan cara merutekan lalu lintas di internet. Dengan zona pribadi yang dihosting, catatan menentukan cara merutekan lalu lintas di VPC Anda.

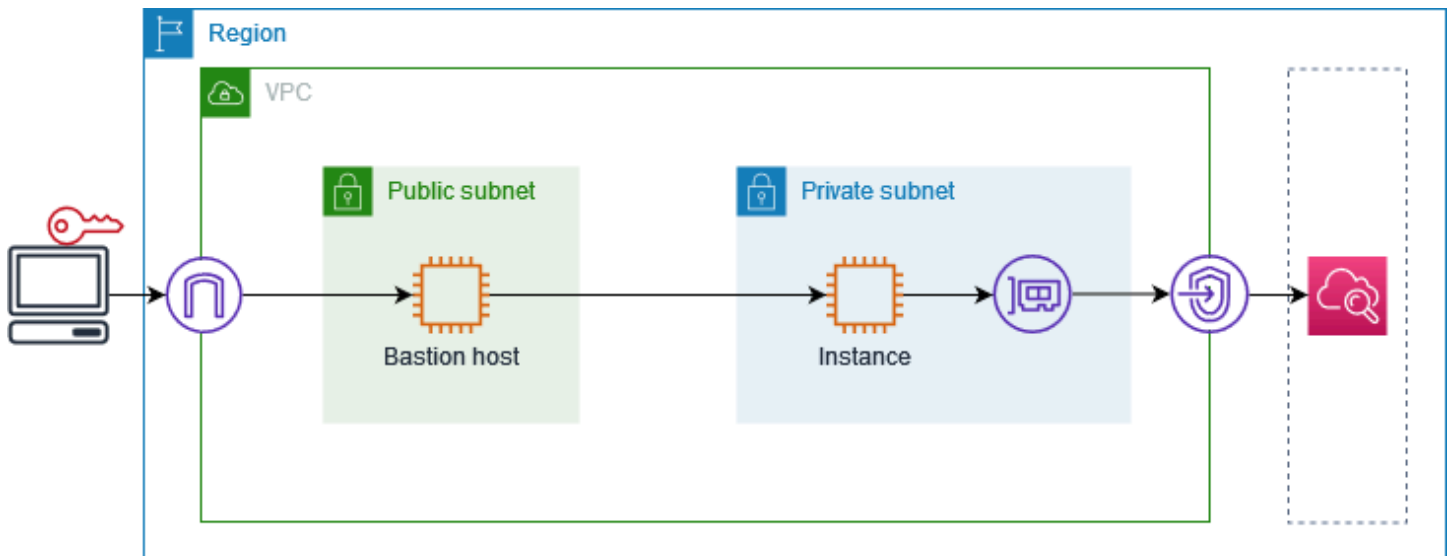
Anda dapat mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas domain ke titik akhir VPC. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke titik akhir VPC menggunakan nama domain Anda](#).

Anda dapat menggunakan Route 53 untuk mengonfigurasi DNS split-horizon, di mana Anda menggunakan nama domain yang sama untuk situs web publik dan layanan titik akhir yang didukung oleh AWS PrivateLink. Permintaan DNS untuk nama host publik dari VPC konsumen diselesaikan ke alamat IP pribadi antarmuka jaringan titik akhir, tetapi permintaan dari luar VPC terus diselesaikan ke titik akhir publik. Untuk informasi selengkapnya, lihat Mekanisme [DNS untuk Perutean Lalu Lintas dan Mengaktifkan Failover untuk Penerapan AWS PrivateLink](#).

Memulai dengan AWS PrivateLink

Tutorial ini menunjukkan cara mengirim permintaan dari instance EC2 di subnet pribadi ke Amazon CloudWatch menggunakan AWS PrivateLink.

Diagram berikut memberikan gambaran umum skenario ini. Untuk terhubung dari komputer Anda ke instance di subnet pribadi, pertama-tama Anda harus terhubung ke host bastion di subnet publik. Baik host bastion maupun instance harus menggunakan pasangan kunci yang sama. Karena .pem file untuk kunci pribadi ada di komputer Anda, bukan host bastion, Anda akan menggunakan penerusan kunci SSH. Kemudian, Anda dapat terhubung ke instance dari host bastion tanpa menentukan .pem file dalam ssh perintah. Setelah Anda menyiapkan titik akhir VPC untuk CloudWatch, lalu lintas dari instans yang ditakdirkan diselesaikan ke antarmuka jaringan titik akhir dan kemudian dikirim ke CloudWatch menggunakan titik akhir VPC. CloudWatch



Untuk tujuan pengujian, Anda dapat menggunakan Zona Ketersediaan tunggal. Dalam produksi, kami menyarankan Anda menggunakan setidaknya dua Zona Ketersediaan untuk latensi rendah dan ketersediaan tinggi.

Tugas

- [Langkah 1: Buat VPC dengan subnet](#)
- [Langkah 2: Luncurkan instance](#)
- [Langkah 3: Uji CloudWatch akses](#)
- [Langkah 4: Buat titik akhir VPC untuk mengakses CloudWatch](#)

- [Langkah 5: Uji titik akhir VPC](#)
- [Langkah 6: Bersihkan](#)

Langkah 1: Buat VPC dengan subnet

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet pribadi.

Untuk membuat VPC

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Pilih Buat VPC.
3. Untuk Sumber Daya yang akan dibuat, pilih VPC dan lainnya.
4. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.
5. Untuk mengkonfigurasi subnet, lakukan hal berikut:
 - a. Untuk Jumlah Zona Ketersediaan, pilih 1 atau 2, tergantung kebutuhan Anda.
 - b. Untuk Jumlah subnet publik, pastikan Anda memiliki satu subnet publik per Zona Ketersediaan.
 - c. Untuk Jumlah subnet pribadi, pastikan Anda memiliki satu subnet pribadi per Zona Ketersediaan.
6. Pilih Buat VPC.

Langkah 2: Luncurkan instance

Menggunakan VPC yang Anda buat pada langkah sebelumnya, luncurkan host bastion di subnet publik dan instance di subnet pribadi.

Prasyarat

- Buat pasangan kunci menggunakan format .pem. Anda harus memilih pasangan kunci ini ketika Anda meluncurkan host bastion dan instance.
- Buat grup keamanan untuk host bastion yang memungkinkan lalu lintas SSH masuk dari blok CIDR untuk komputer Anda.
- Buat grup keamanan untuk instance yang memungkinkan lalu lintas SSH masuk dari grup keamanan untuk host bastion.

- Buat profil instance IAM dan lampirkan CloudWatchReadOnlyAccess kebijakan.

Untuk meluncurkan tuan rumah benteng

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
2. Pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk host benteng Anda.
4. Pertahankan gambar default dan jenis instance.
5. Untuk Pasangan kunci, pilih pasangan kunci Anda.
6. Untuk Pengaturan jaringan, lakukan hal berikut:
 - a. Untuk VPC, pilih VPC Anda.
 - b. Untuk Subnet, pilih subnet publik.
 - c. Untuk IP Auto-assign publik, pilih Aktifkan.
 - d. Untuk Firewall, pilih Pilih grup keamanan yang ada dan kemudian pilih grup keamanan untuk host bastion.
7. Pilih Luncurkan instans.

Untuk meluncurkan instance

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
2. Pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk instance Anda.
4. Pertahankan gambar default dan jenis instance.
5. Untuk Pasangan kunci, pilih pasangan kunci Anda.
6. Untuk Pengaturan jaringan, lakukan hal berikut:
 - a. Untuk VPC, pilih VPC Anda.
 - b. Untuk Subnet, pilih subnet pribadi.
 - c. Untuk IP Auto-assign publik, pilih Non aktifkan.
 - d. Untuk Firewall, pilih Pilih grup keamanan yang ada dan kemudian pilih grup keamanan untuk instance tersebut.
7. Perluas detail lanjutan. Untuk profil instans IAM, pilih profil instans IAM Anda.

8. Pilih Luncurkan instans.

Langkah 3: Uji CloudWatch akses

Gunakan prosedur berikut untuk mengonfirmasi bahwa instance tidak dapat mengakses CloudWatch. Anda akan melakukannya menggunakan AWS CLI perintah read-only untuk. CloudWatch

Untuk menguji CloudWatch akses

1. Dari komputer Anda, tambahkan pasangan kunci ke agen SSH menggunakan perintah berikut, di *key.pem* mana nama file.pem Anda.

```
ssh-add ./key.pem
```

Jika Anda menerima kesalahan bahwa izin untuk pasangan kunci Anda terlalu terbuka, jalankan perintah berikut, lalu coba lagi perintah sebelumnya.

```
chmod 400 ./key.pem
```

2. Hubungkan ke host benteng dari komputer Anda. Anda harus menentukan -A opsi, nama pengguna instance (misalnya,ec2-user), dan alamat IP publik dari host bastion.

```
ssh -A ec2-user@bastion-public-ip-address
```

3. Hubungkan ke instance dari host benteng. Anda harus menentukan nama pengguna instance (misalnya,ec2-user) dan alamat IP pribadi dari instance.

```
ssh ec2-user@instance-private-ip-address
```

4. Jalankan [perintah CloudWatch](#) list-metrics pada instance sebagai berikut. Untuk --region opsi, tentukan Wilayah tempat Anda membuat VPC.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

5. Setelah beberapa menit, perintah habis. Ini menunjukkan bahwa Anda tidak dapat mengakses CloudWatch dari instance dengan konfigurasi VPC saat ini.

```
Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
```

6. Tetap terhubung dengan instans Anda. Setelah Anda membuat titik akhir VPC, Anda akan mencoba list-metrics perintah ini lagi.

Langkah 4: Buat titik akhir VPC untuk mengakses CloudWatch

Gunakan prosedur berikut untuk membuat titik akhir VPC yang terhubung ke CloudWatch.

Prasyarat

Buat grup keamanan untuk titik akhir VPC yang memungkinkan lalu lintas ke CloudWatch. Misalnya, tambahkan aturan yang memungkinkan lalu lintas HTTPS dari blok VPC CIDR.

Untuk membuat titik akhir VPC untuk CloudWatch

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Tag nama, masukkan nama untuk titik akhir.
5. Untuk Kategori layanan, pilih Layanan AWS.
6. Untuk Layanan, pilih `com.amazonaws.region.pemantauan`.
7. Untuk VPC, pilih VPC Anda.
8. Untuk Subnet, pilih Availability Zone dan kemudian pilih subnet pribadi.
9. Untuk grup keamanan, pilih grup keamanan untuk titik akhir VPC.
10. Untuk Kebijakan, pilih Akses penuh untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya melalui titik akhir VPC.
11. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
12. Pilih Buat titik akhir. Status awal adalah Tertunda. Sebelum Anda pergi ke langkah berikutnya, tunggu sampai status Tersedia. Hal ini dapat menghabiskan waktu beberapa menit.

Langkah 5: Uji titik akhir VPC

Verifikasi bahwa titik akhir VPC mengirim permintaan dari instance Anda ke CloudWatch.

Untuk menguji titik akhir VPC

Jalankan perintah berikut di instans Anda. Untuk `--region` opsi, tentukan Wilayah tempat Anda membuat titik akhir VPC.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

Jika Anda mendapatkan respons, bahkan respons dengan hasil kosong, maka Anda terhubung untuk CloudWatch menggunakan AWS PrivateLink.

Jika Anda mendapatkan `UnauthorizedOperation` kesalahan, pastikan bahwa instance memiliki peran IAM yang memungkinkan akses ke CloudWatch.

Jika permintaan habis waktu, verifikasi hal berikut:

- Grup keamanan untuk titik akhir memungkinkan lalu lintas ke CloudWatch.
- `--region` Opsi menentukan Wilayah tempat Anda membuat titik akhir VPC.

Langkah 6: Bersihkan

Jika Anda tidak lagi membutuhkan host bastion dan instance yang Anda buat untuk tutorial ini, Anda dapat menghentikannya.

Untuk mengakhirkan instans

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Instans.
3. Pilih kedua instance pengujian dan pilih Status Instance, Hentikan instance.
4. Saat diminta konfirmasi, pilih Akhiri.

Jika Anda tidak lagi memerlukan titik akhir VPC, Anda dapat menghapusnya.

Untuk menghapus titik akhir VPC

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir VPC.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

Akses Layanan AWS lewat AWS PrivateLink

Anda mengakses Layanan AWS menggunakan titik akhir. Titik akhir layanan default adalah antarmuka publik, jadi Anda harus menambahkan gateway internet ke VPC Anda sehingga lalu lintas dapat masuk dari VPC ke Layanan AWS. Jika konfigurasi ini tidak berfungsi dengan persyaratan keamanan jaringan Anda, Anda dapat menggunakannya AWS PrivateLink untuk menghubungkan VPC Anda Layanan AWS seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet.

Anda dapat mengakses secara pribadi Layanan AWS yang terintegrasi dengan AWS PrivateLink menggunakan titik akhir VPC. Anda dapat membangun dan mengelola semua lapisan tumpukan aplikasi Anda tanpa menggunakan gateway internet.

Harga

Anda ditagih untuk setiap jam titik akhir VPC antarmuka Anda disediakan di setiap Zona Ketersediaan. Anda juga ditagih per GB data yang diproses. Untuk informasi selengkapnya, silakan lihat [AWS PrivateLink Harga](#).

Daftar Isi

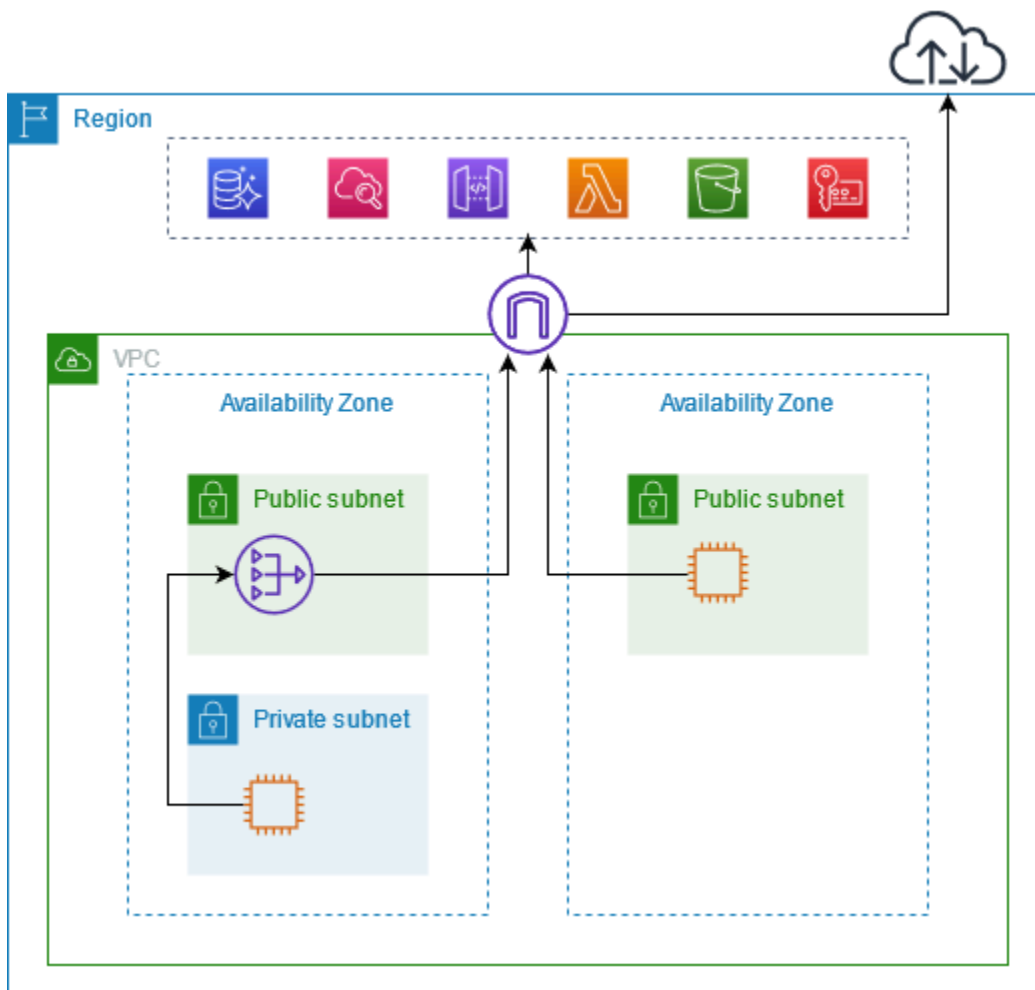
- [Gambaran umum](#)
- [Nama host DNS](#)
- [Resolusi DNS](#)
- [DNS privat](#)
- [Subnet dan Zona Ketersediaan](#)
- [Jenis alamat IP](#)
- [Jenis IP catatan DNS](#)
- [Layanan AWS yang berintegrasi dengan AWS PrivateLink](#)
- [Cross-region diaktifkan Layanan AWS](#)
- [Akses Layanan AWS menggunakan antarmuka titik akhir VPC](#)
- [Konfigurasi titik akhir antarmuka](#)
- [Menerima peringatan untuk peristiwa titik akhir antarmuka](#)
- [Menghapus titik akhir antarmuka](#)
- [Titik akhir Gateway](#)

Gambaran umum

Anda dapat mengakses Layanan AWS melalui titik akhir layanan publik mereka atau terhubung ke penggunaan yang didukung Layanan AWS . AWS PrivateLink Ikhtisar ini membandingkan metode ini.

Akses melalui titik akhir layanan publik

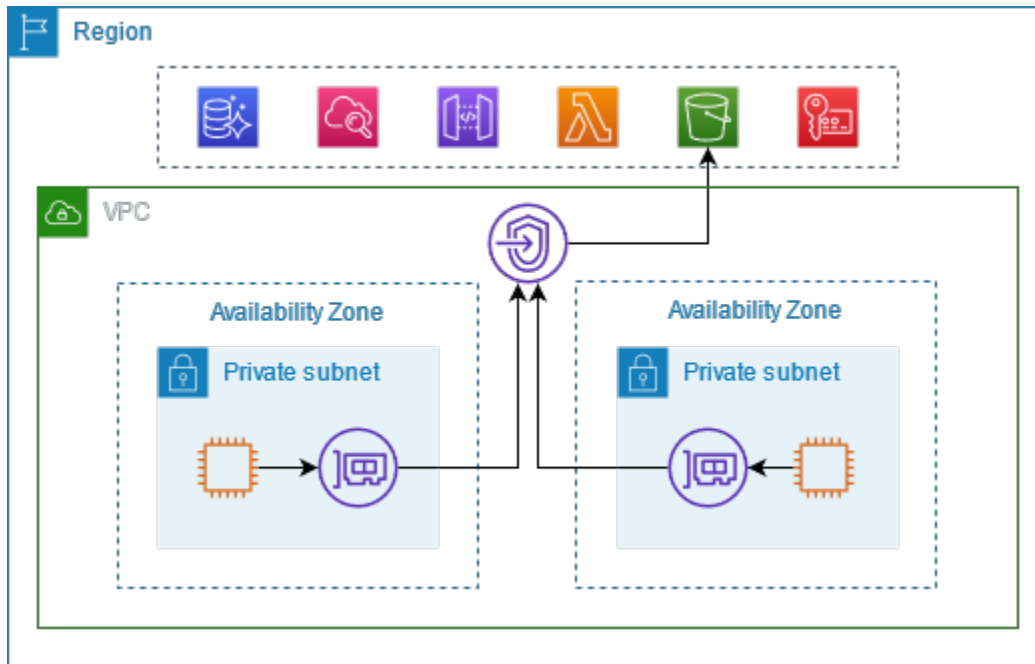
Diagram berikut menunjukkan bagaimana instance mengakses Layanan AWS melalui titik akhir layanan publik. Lalu lintas ke instans di subnet publik dialihkan ke gateway internet untuk VPC dan kemudian ke. Layanan AWS Layanan AWS Lalu lintas ke instans di subnet pribadi dialihkan ke gateway NAT, lalu ke gateway internet untuk VPC, dan kemudian ke. Layanan AWS Layanan AWS Sementara lalu lintas ini melintasi gateway internet, itu tidak meninggalkan AWS jaringan.



Hubungkan melalui AWS PrivateLink

Diagram berikut menunjukkan bagaimana instance mengakses Layanan AWS melalui AWS PrivateLink. Pertama, Anda membuat antarmuka titik akhir VPC, yang membuat koneksi antara

subnet di VPC Anda dan antarmuka jaringan yang Layanan AWS menggunakan. Lalu lintas yang Layanan AWS ditujukan untuk diselesaikan ke alamat IP pribadi dari antarmuka jaringan titik akhir menggunakan DNS, dan kemudian dikirim ke Layanan AWS menggunakan koneksi antara titik akhir VPC dan Layanan AWS



Layanan AWS menerima permintaan koneksi secara otomatis. Layanan tidak dapat memulai permintaan ke sumber daya melalui titik akhir VPC.

Nama host DNS

Sebagian besar Layanan AWS menawarkan titik akhir Regional publik, yang memiliki sintaks berikut.

```
protocol://service_code.region_code.amazonaws.com
```

Misalnya, titik akhir publik untuk Amazon CloudWatch di us-east-2 adalah sebagai berikut.

```
https://monitoring.us-east-2.amazonaws.com
```

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke layanan menggunakan titik akhir pribadi. Saat Anda membuat titik akhir VPC antarmuka, kami membuat nama DNS Regional dan zonal yang dapat Anda gunakan untuk berkomunikasi dengan Layanan AWS dari VPC Anda.

Nama DNS Regional untuk titik akhir VPC antarmuka Anda memiliki sintaks berikut:

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

Nama DNS zonal memiliki sintaks berikut:

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

Saat Anda membuat titik akhir VPC antarmuka untuk sebuah Layanan AWS, Anda dapat mengaktifkan DNS [???](#) pribadi. Dengan DNS pribadi, Anda dapat terus membuat permintaan ke layanan menggunakan nama DNS untuk titik akhir publiknya, sambil memanfaatkan konektivitas pribadi melalui antarmuka titik akhir VPC. Untuk informasi selengkapnya, lihat [the section called “Resolusi DNS”](#).

Perintah [describe-vpc-endpoints](#) berikut menampilkan entri DNS untuk titik akhir antarmuka.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
VpcEndpoints[*].DnsEntries
```

Berikut ini adalah contoh output untuk titik akhir antarmuka untuk Amazon CloudWatch dengan nama DNS pribadi diaktifkan. Entri pertama adalah titik akhir Regional pribadi. Tiga entri berikutnya adalah titik akhir zona pribadi. Entri terakhir berasal dari zona host pribadi tersembunyi, yang menyelesaikan permintaan ke titik akhir publik ke alamat IP pribadi dari antarmuka jaringan titik akhir.

```
[
  [
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
```

```
    "DnsName": "vpce-099deb00b40f00e22-1j2wisx3-us-east-2b.monitoring.us-east-2.vpce.amazonaws.com",
    "HostedZoneId": "ZC8PG0KIFKBRI"
  },
  {
    "DnsName": "monitoring.us-east-2.amazonaws.com",
    "HostedZoneId": "Z06320943MM0WYG6MAVL9"
  }
]
```

Resolusi DNS

Catatan DNS yang kami buat untuk titik akhir VPC antarmuka Anda bersifat publik. Oleh karena itu, nama-nama DNS ini dapat diselesaikan secara publik. Namun, permintaan DNS dari luar VPC masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir, sehingga alamat IP ini tidak dapat digunakan untuk mengakses layanan titik akhir kecuali Anda memiliki akses ke VPC.

DNS privat

Jika Anda mengaktifkan DNS pribadi untuk titik akhir VPC antarmuka Anda, dan VPC Anda mengaktifkan nama [host DNS dan resolusi](#) DNS, kami membuat zona pribadi yang AWS dikelola dan tersembunyi untuk Anda. Zona yang dihosting berisi kumpulan rekaman untuk nama DNS default untuk layanan yang menyelesaikannya ke alamat IP pribadi antarmuka jaringan titik akhir di VPC Anda. Oleh karena itu, jika Anda memiliki aplikasi yang sudah ada yang mengirim permintaan ke Layanan AWS menggunakan titik akhir Regional publik, permintaan tersebut sekarang melewati antarmuka jaringan titik akhir, tanpa mengharuskan Anda membuat perubahan apa pun pada aplikasi tersebut.

Sebaiknya aktifkan nama DNS pribadi untuk titik akhir VPC Anda untuk. Layanan AWS Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik akhir VPC Anda.

Amazon menyediakan server DNS untuk VPC Anda, yang disebut [Route 53 Resol](#) ver. Route 53 Resolver secara otomatis menyelesaikan nama domain VPC lokal dan rekaman di zona yang dihosting pribadi. Namun, Anda tidak dapat menggunakan Route 53 Resolver dari luar VPC Anda. Jika Anda ingin mengakses titik akhir VPC dari jaringan lokal, Anda dapat menggunakan titik akhir Route 53 Resolver dan aturan Resolver. Untuk informasi selengkapnya, lihat [Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver](#).

Subnet dan Zona Ketersediaan

Anda dapat mengonfigurasi titik akhir VPC Anda dengan satu subnet per Zona Ketersediaan. Kami membuat antarmuka jaringan titik akhir untuk titik akhir VPC di subnet Anda. Kami menetapkan alamat IP ke setiap antarmuka jaringan titik akhir dari subnetnya, berdasarkan jenis alamat [IP](#) dari titik akhir VPC. Alamat IP antarmuka jaringan titik akhir tidak akan berubah selama masa pakai titik akhir VPC-nya.

Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, kami merekomendasikan hal berikut:

- Konfigurasi setidaknya dua Zona Ketersediaan per titik akhir VPC dan gunakan AWS sumber daya Anda yang harus mengakses Layanan AWS di Zona Ketersediaan ini.
- Konfigurasi nama DNS pribadi untuk titik akhir VPC.
- Akses Layanan AWS dengan menggunakan nama DNS Regional, juga dikenal sebagai titik akhir publik.

Diagram berikut menunjukkan titik akhir VPC untuk Amazon CloudWatch dengan antarmuka jaringan titik akhir dalam Zona Ketersediaan tunggal. Ketika sumber daya apa pun di subnet mana pun di VPC mengakses Amazon CloudWatch menggunakan titik akhir publiknya, kami menyelesaikan lalu lintas ke alamat IP antarmuka jaringan titik akhir. Ini termasuk lalu lintas dari subnet di Zona Ketersediaan lainnya. Namun, jika Zona Ketersediaan 1 terganggu, sumber daya di Zona Ketersediaan 2 kehilangan akses ke Amazon CloudWatch.

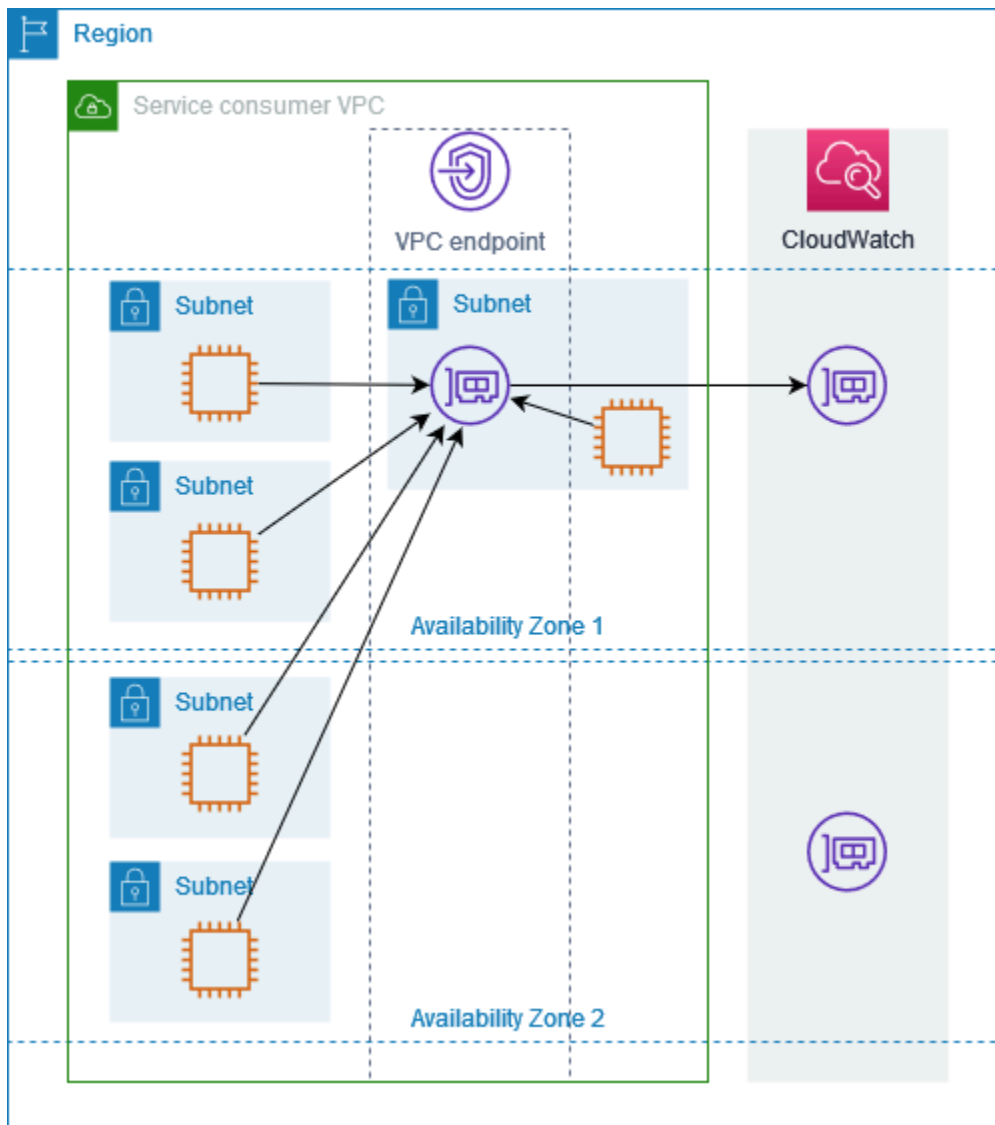
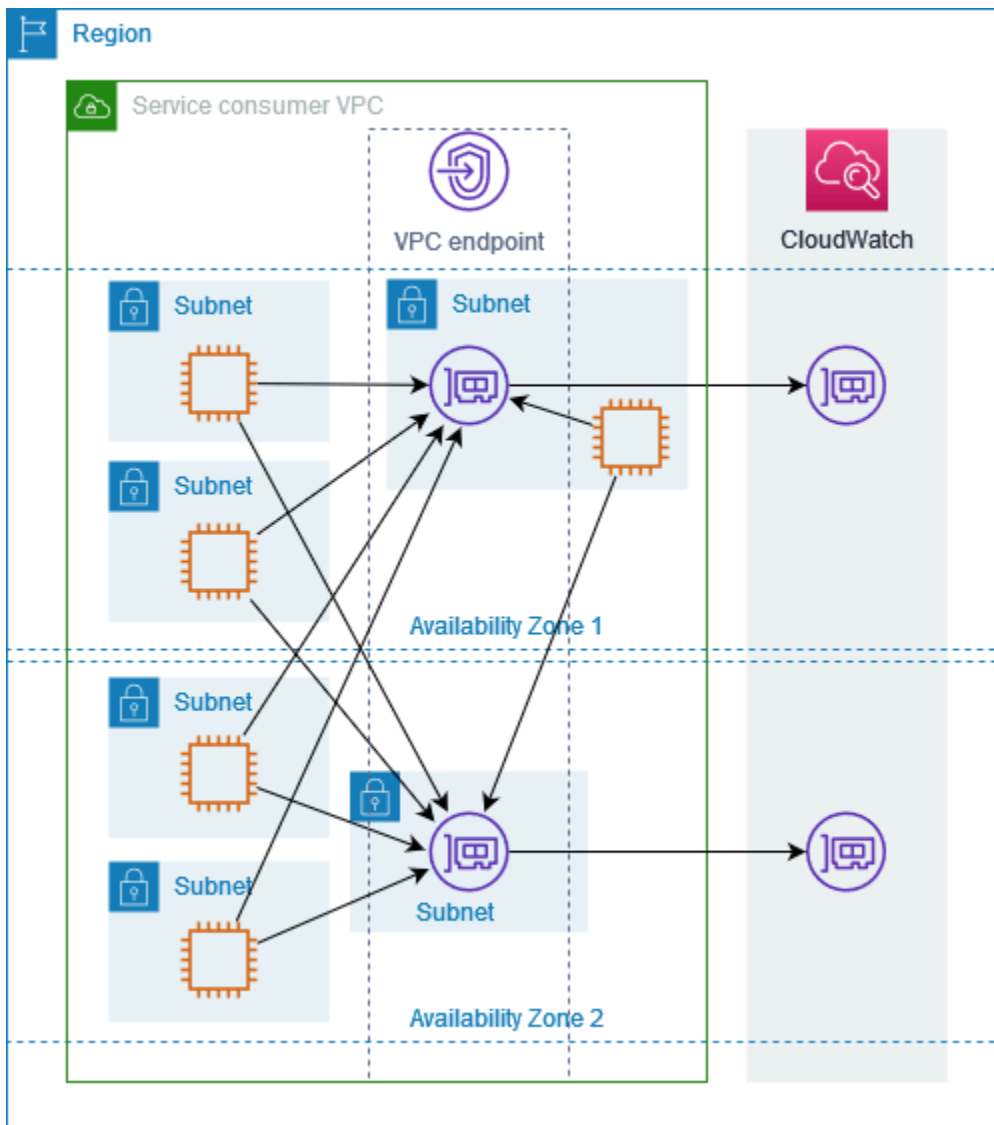
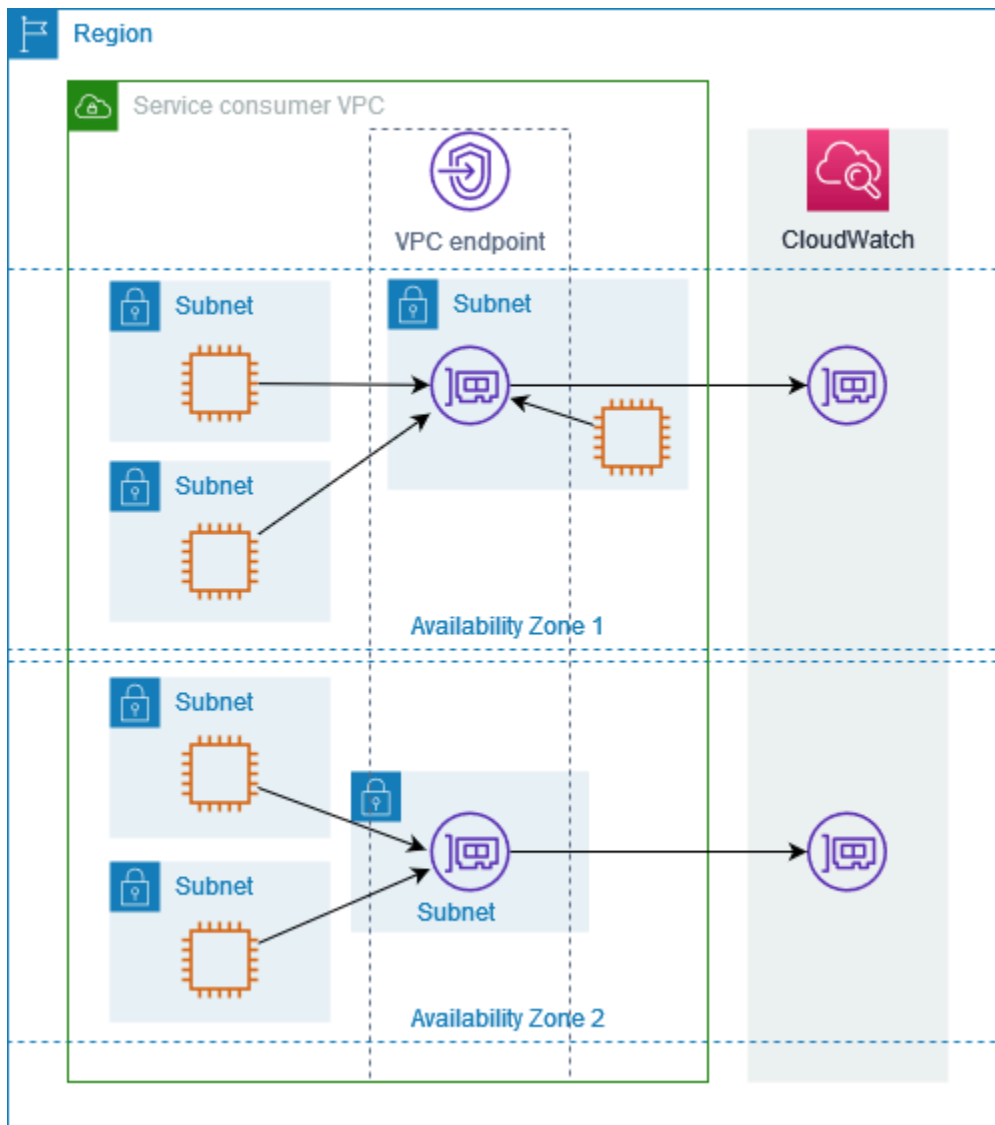


Diagram berikut menunjukkan titik akhir VPC untuk Amazon CloudWatch dengan antarmuka jaringan titik akhir di dua Zona Ketersediaan. Ketika sumber daya apa pun di subnet mana pun di VPC mengakses Amazon CloudWatch dengan menggunakan titik akhir publiknya, kami memilih antarmuka jaringan titik akhir yang sehat, menggunakan algoritma round robin untuk bergantian di antara keduanya. Kami kemudian menyelesaikan lalu lintas ke alamat IP dari antarmuka jaringan titik akhir yang dipilih.



Jika lebih baik untuk kasus penggunaan Anda, Anda dapat mengirim lalu lintas dari sumber daya Anda ke Layanan AWS dengan menggunakan antarmuka jaringan titik akhir di Zona Ketersediaan yang sama. Untuk melakukannya, gunakan titik akhir zonal pribadi atau alamat IP dari antarmuka jaringan titik akhir.



Jenis alamat IP

Layanan AWS dapat mendukung IPv6 melalui titik akhir pribadi mereka bahkan jika mereka tidak mendukung IPv6 melalui titik akhir publik mereka. Endpoint yang mendukung IPv6 dapat menanggapi kueri DNS dengan catatan AAAA.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir antarmuka

- Layanan AWS Harus membuat titik akhir layanannya tersedia melalui IPv6. Untuk informasi selengkapnya, lihat [the section called “Lihat dukungan IPv6”](#).
- Jenis alamat IP dari titik akhir antarmuka harus kompatibel dengan subnet untuk titik akhir antarmuka, seperti yang dijelaskan di sini:

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

Jika antarmuka titik akhir VPC mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika antarmuka titik akhir VPC mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan titik akhir tidak dapat dijangkau dari internet. Jika Anda menjelaskan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Jenis IP catatan DNS

Tergantung pada jenis alamat IP Anda, ketika Anda memanggil titik akhir VPC, AWS layanan dapat mengembalikan catatan A, catatan AAAA, atau catatan A dan AAAA. Anda dapat menyesuaikan jenis rekaman yang dikem AWS balikan layanan Anda dengan memodifikasi jenis IP catatan DNS. Tabel berikut menunjukkan jenis IP catatan DNS yang didukung dan jenis rekaman yang dikembalikan:

Jenis IP catatan DNS	Jenis rekaman yang dikembalikan
IPv4	A
IPv6	AAAA
Tumpukan ganda	A dan AAAA

Secara default, jenis catatan DNS sama dengan jenis alamat IP. Anda dapat memilih jenis IP catatan DNS yang berbeda, tetapi Anda harus menggunakan jenis alamat IP yang kompatibel untuk layanan titik akhir. Tabel berikut menunjukkan jenis IP catatan DNS yang didukung untuk setiap jenis alamat IP untuk titik akhir antarmuka:

Jenis alamat IP	Jenis IP catatan DNS yang didukung
IPv4	IPv4

Jenis alamat IP	Jenis IP catatan DNS yang didukung
IPv6	IPv6
Tumpukan ganda	Dualstack*, IPv4, IPv6, ditentukan layanan

* Merupakan tipe IP catatan DNS default.

Jenis IP catatan DNS yang ditentukan layanan mengembalikan catatan DNS berdasarkan titik akhir layanan yang Anda panggil. Jika Anda menggunakan jenis IP catatan DNS yang ditentukan layanan, pastikan layanan Anda dapat menangani panggilan variabel dari titik akhir layanan. Untuk melihat catatan DNS yang didukung oleh titik akhir antarmuka Anda, lihat nama DNS untuk titik akhir VPC Anda di Konsol Manajemen AWS, atau gunakan [DescribeVpcEndpoints](#).

Perilaku tipe IP catatan DNS berbeda untuk titik akhir gateway. Untuk informasi selengkapnya, lihat [Jenis IP catatan DNS untuk titik akhir gateway](#).

Layanan AWS yang berintegrasi dengan AWS PrivateLink

Berikut ini ter Layanan AWS integrasi dengan AWS PrivateLink. Anda dapat membuat titik akhir VPC untuk terhubung ke layanan ini secara pribadi, seolah-olah mereka berjalan di VPC Anda sendiri.

Pilih tautan di Layanan AWS kolom untuk melihat dokumentasi untuk layanan yang terintegrasi dengan AWS PrivateLink. Kolom Nama layanan berisi nama layanan yang Anda tentukan saat membuat antarmuka titik akhir VPC, atau menunjukkan bahwa layanan mengelola titik akhir.

Layanan AWS	Nama layanan
AWS Account Management	com.amazonaws. <i>region</i> .akun
Amazon API Gateway	com.amazonaws. <i>region</i> .eksekusi api com.amazonaws. <i>region</i> .apigateway
AWS AppConfig	com.amazonaws. <i>region</i> .appconfig com.amazonaws. <i>region</i> .appconfig-fips com.amazonaws. <i>region</i> .appconfigdata

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .appconfigdata-fips
AWS App Mesh	com.amazonaws. <i>region</i> .aplikasi mesh
	com.amazonaws. <i>region</i> .appmesh-envoy-manajemen
AWS Pelari Aplikasi	com.amazonaws. <i>region</i> .appruner
AWS Layanan App Runner	com.amazonaws. <i>region</i> .apprunner.request
Penskalaan Otomatis Aplikasi	com.amazonaws. <i>region</i> .aplikasi-penskalaan otomatis
AWS Application Discovery Service	com.amazonaws. <i>region</i> .penemuan
	com.amazonaws. <i>region</i> .penemuan persenjataan
AWS Layanan Migrasi Aplikasi	com.amazonaws. <i>region</i> .mgn
WorkSpaces Aplikasi Amazon	com.amazonaws. <i>region</i> .appstream.api
	com.amazonaws. <i>region</i> .appstream.streaming
AWS AppSync	com.amazonaws. <i>region</i> .appsync-api
Amazon Athena	com.amazonaws. <i>region</i> .athena
AWS Audit Manager	com.amazonaws. <i>region</i> .manajer audit
Amazon Aurora	com.amazonaws. <i>region</i> .rds
	com.amazonaws. <i>region</i> .rds-fips
Amazon Aurora DSQL	com.amazonaws. <i>region</i> .dsql
AWS Auto Scaling	com.amazonaws. <i>region</i> .rencana penskalaan otomatis
AWS Pertukaran Data B2B	com.amazonaws. <i>region</i> .b2bi
AWS Backup	com.amazonaws. <i>region</i> .cadangan

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .backup-gateway
AWS Batch	com.amazonaws. <i>region</i> .batch
Amazon Bedrock	com.amazonaws. <i>region</i> .batuan dasar
	com.amazonaws. <i>region</i> .bedrock-agen
	com.amazonaws. <i>region</i> .bedrock-agen-runtime
	com.amazonaws. <i>region</i> .bedrock-data-otomatisasi
	com.amazonaws. <i>region</i> .bedrock-data-automasi-fips
	com.amazonaws. <i>region</i> .bedrock-data-automasi-runtime
	com.amazonaws. <i>region</i> .bedrock-data-automasi-runtime-fips
	com.amazonaws. <i>region</i> .bedrock-runtime
Amazon Bedrock AgentCore	com.amazonaws. <i>region</i> .bedrock-agentcore-kontrol
	com.amazonaws. <i>region</i> .bedrock-agentcore
AWS Manajemen Penagihan dan Biaya	com.amazonaws. <i>region</i> .penagihan
	com.amazonaws. <i>region</i> .freetier
	com.amazonaws. <i>region</i> .pajak
AWS Billing Conductor	com.amazonaws. <i>region</i> .tagihan konduktor
Amazon Bracket	com.amazonaws. <i>region</i> .braket
AWS Certificate Manager	com.amazonaws. <i>region</i> .acm
	com.amazonaws. <i>region</i> .acm-fips

Layanan AWS	Nama layanan
Amazon Chime SDK	com.amazonaws. <i>region</i> .chime-sdk-suara
	com.amazonaws. <i>region</i> .rapat-lonceng
	com.amazonaws. <i>region</i> .messaging-chime
	com.amazonaws. <i>region</i> .messaging-chime-fips
	com.amazonaws. <i>region</i> .identiti-lonceng
	com.amazonaws. <i>region</i> .identity-chime-fips
	com.amazonaws. <i>region</i> .media-pipelines-lonceng
	com.amazonaws. <i>region</i> .media-pipelines-chime-fips
AWS Kamar Bersih	com.amazonaws. <i>region</i> .kamar mandi
	com.amazonaws. <i>region</i> .cleanrooms-fips
AWS Kamar Bersih ML	com.amazonaws. <i>region</i> .cleanroom-ML
AWS Cloud Control API	com.amazonaws. <i>region</i> .cloud controlapi
	com.amazonaws. <i>region</i> .cloudcontrolapi-fips
Direktori Amazon Cloud	com.amazonaws. <i>region</i> .clouddirektori
AWS CloudFormation	com.amazonaws. <i>region</i> .formasi awan
	com.amazonaws. <i>region</i> .cloudformation-fips
Amazon CloudFront	com.amazonaws.cloudfront
Paket CloudFront Flat-Rate Harga Amazon	com.amazonaws.us-east-1.pricingplanmanager
AWS CloudHSM	com.amazonaws. <i>region</i> .cloudhsmv2
AWS Cloud Map	com.amazonaws. <i>region</i> .layanan iscovery

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .servicediscovery-fips
	com.amazonaws. <i>region</i> .data-servicediscovery
	com.amazonaws. <i>region</i> .data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. <i>region</i> .cloud trail
AWS Cloud WAN	com.amazonaws. <i>region</i> .manajer jaringan
Amazon CloudWatch	com.amazonaws. <i>region</i> .aplikasi-sinyal
	com.amazonaws. <i>region</i> .wawasan aplikasi
	com.amazonaws. <i>region</i> .monitor internet
	com.amazonaws. <i>region</i> .internetmonitor-fips
	com.amazonaws. <i>region</i> .pemantauan
	com.amazonaws. <i>region</i> .monitor aliran jaringan
	com.amazonaws. <i>region</i> .networkflowmonitorreport
	com.amazonaws. <i>region</i> .monitor jaringan
	com.amazonaws. <i>region</i> .observabilityadmin
	com.amazonaws. <i>region</i> .rum
	com.amazonaws. <i>region</i> .rum-dataplane
	com.amazonaws. <i>region</i> .sintetis
	com.amazonaws. <i>region</i> .sintetis-fips
	com.amazonaws. <i>region</i> .oam
CloudWatch Log Amazon	com.amazonaws. <i>region</i> .log

Layanan AWS	Nama layanan
AWS CodeArtifact	com.amazonaws. <i>region</i> .codeartifact.api com.amazonaws. <i>region</i> .codeartifact.repositori
AWS CodeBuild	com.amazonaws. <i>region</i> .codebuild com.amazonaws. <i>region</i> .codebuild-fips
AWS CodeCommit	com.amazonaws. <i>region</i> .codedekomit com.amazonaws. <i>region</i> .codecommit-fips com.amazonaws. <i>region</i> .git-codedekomit com.amazonaws. <i>region</i> .git-codecommit-fips
AWS CodeConnections	com.amazonaws. <i>region</i> .codeconnections.api com.amazonaws. <i>region</i> .kodestar-koneksi.api
AWS CodeDeploy	com.amazonaws. <i>region</i> .codedeploy com.amazonaws. <i>region</i> .codedeploy-perintah-aman com.amazonaws. <i>region</i> .codedeploy-fips
CodeGuru Profiler Amazon	com.amazonaws. <i>region</i> .codeguru profil
Pengulas CodeGuru Amazon	com.amazonaws. <i>region</i> .codeguru-pengulas
AWS CodePipeline	com.amazonaws. <i>region</i> .codepipeline
Amazon Comprehend	com.amazonaws. <i>region</i> .commenangkap com.amazonaws. <i>region</i> .comprehend-fips
Amazon Comprehend Medical	com.amazonaws. <i>region</i> .comprehendmedis
AWS Compute Optimizer	com.amazonaws. <i>region</i> .komput-pengoptimal

Layanan AWS	Nama layanan
AWS Config	com.amazonaws. <i>region</i> .konfigurasi
	com.amazonaws. <i>region</i> .config-fips
Hubungkan Pelanggan	com.amazonaws. <i>region</i> .app-integrasi
	com.amazonaws. <i>region</i> .kasus
	com.amazonaws. <i>region</i> .sambungkan
	com.amazonaws. <i>region</i> .connect-fips
	com.amazonaws. <i>region</i> .connect-kampanye
	com.amazonaws. <i>region</i> .profil
	com.amazonaws. <i>region</i> .id suara
	com.amazonaws. <i>region</i> .kebijaksanaan
AWS Connector Service	com.amazonaws. <i>region</i> .awskonektor
AWS Katalog Kontrol	com.amazonaws. <i>region</i> .controlkatalog
AWS Cost Explorer	com.amazonaws. <i>region</i> .ce
Hub Optimisasi Biaya AWS	com.amazonaws. <i>region</i> .hub pengoptimalan biaya
AWS Control Tower	com.amazonaws. <i>region</i> .menara kontrol
	com.amazonaws. <i>region</i> .controltower-fips
AWS Data Exchange	com.amazonaws. <i>region</i> .pertukaran data
Ekspor Data AWS	aws.api. <i>region</i> .bcm-data-ekspor
	com.amazonaws. <i>region</i> .bcm-kalkulator harga
Selang Api Data Amazon	com.amazonaws. <i>region</i> .kinesis-firehose

Layanan AWS	Nama layanan
Amazon Data Lifecycle Manager	com.amazonaws. <i>region</i> .dlm com.amazonaws. <i>region</i> .dlm-fips
AWS Database Migration Service	com.amazonaws. <i>region</i> .dms com.amazonaws. <i>region</i> .dms-fips
AWS DataSync	com.amazonaws. <i>region</i> .datasync
Amazon DataZone	com.amazonaws. <i>region</i> .data zone com.amazonaws. <i>region</i> .datazone-fips
AWS Deadline Cloud	com.amazonaws. <i>region</i> .deadline.manajemen com.amazonaws. <i>region</i> .deadline.penjadwalan
Amazon Detective	com.amazonaws. <i>region</i> .detektif com.amazonaws. <i>region</i> .detective-fips
Amazon DevOps Guru	com.amazonaws. <i>region</i> .devops-guru
AWS Direct Connect	com.amazonaws. <i>region</i> .koneksi langsung com.amazonaws. <i>region</i> .directconnect-fips
AWS Directory Service	com.amazonaws. <i>region</i> .ds com.amazonaws. <i>region</i> .ds-data com.amazonaws. <i>region</i> .ds-data-fips
Amazon DocumentDB	com.amazonaws. <i>region</i> .rds
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb com.amazonaws. <i>region</i> .dynamodb-fips

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .dynamodb-stream
API langsung Amazon EBS	com.amazonaws. <i>region</i> .ebs
	com.amazonaws. <i>region</i> .ebs-fips
Amazon EC2	com.amazonaws. <i>region</i> .ec2
	com.amazonaws. <i>region</i> .ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws. <i>region</i> .penskalaan otomatis
	com.amazonaws. <i>region</i> .autoscaling-fips
EC2 Image Builder	com.amazonaws. <i>region</i> .pembuat gambar
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
Amazon ECS	com.amazonaws. <i>region</i> .ecs
	com.amazonaws. <i>region</i> .ecs-agen
	com.amazonaws. <i>region</i> .ecs-telemetry
Amazon EX	com.amazonaws. <i>region</i> .ex
	com.amazonaws. <i>region</i> .eks autentikasi
	com.amazonaws. <i>region</i> .eks-fips
	com.amazonaws. <i>region</i> .eks-mcp
	com.amazonaws. <i>region</i> .eks proksi
	com.amazonaws. <i>region</i> .oidc-ex
AWS Elastic Beanstalk	com.amazonaws. <i>region</i> .tangkai kacang elastis

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .elasticbeanstalk-kesehatan
AWS Elastic Disaster Recovery	com.amazonaws. <i>region</i> .drs
Sistem File Elastis Amazon	com.amazonaws. <i>region</i> .sistem file elastik
	com.amazonaws. <i>region</i> .elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. <i>region</i> .penyeimbangan beban elastis
Layanan VMware Amazon Elastic	com.amazonaws. <i>region</i> .EVs
	com.amazonaws. <i>region</i> .evs-fips
Amazon ElastiCache	com.amazonaws. <i>region</i> .elastik
	com.amazonaws. <i>region</i> .elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. <i>region</i> .mediaConnect
AWS Elemental MediaConvert	com.amazonaws. <i>region</i> .mediakonvert
	com.amazonaws. <i>region</i> .mediaconvert-fips
Amazon EMR	com.amazonaws. <i>region</i> .elasticmapreduce
	com.amazonaws. <i>region</i> .elasticmapreduce-fips
	com.amazonaws. <i>region</i> .emr-dasbor
Amazon EMR di EKS	com.amazonaws. <i>region</i> .emr-kontainer
Amazon EMR Tanpa Server	com.amazonaws. <i>region</i> .emr-tanpa server
	com.amazonaws. <i>region</i> .emr-serverless-layanan.livy
	com.amazonaws. <i>region</i> .emr-tanpa server.dasbor
Amazon EMR WAL	com.amazonaws. <i>region</i> .emrwal.prod

Layanan AWS	Nama layanan
AWS Pesan Soal Pengguna Akhir	com.amazonaws. <i>region</i> .pesan sosial
	com.amazonaws. <i>region</i> .social messaging-fips
Resolusi Entitas AWS	com.amazonaws. <i>region</i> .resolusi entitas
	com.amazonaws. <i>region</i> .entityresolution-fips
Amazon EventBridge	com.amazonaws. <i>region</i> .acara
	com.amazonaws. <i>region</i> .event-fips
	com.amazonaws. <i>region</i> .pipa
	com.amazonaws. <i>region</i> .pipes-data
	com.amazonaws. <i>region</i> .pipes-fips
	com.amazonaws. <i>region</i> .skema
Pen EventBridge jadwal Amazon	com.amazonaws. <i>region</i> .penjadwal
AWS Fault Injection Service	com.amazonaws. <i>region</i> .fish
	com.amazonaws. <i>region</i> .fis-fips
Amazon FinSpace	com.amazonaws. <i>region</i> .finspace
	com.amazonaws. <i>region</i> .finspace-api
AWS Firewall Manager	com.amazonaws. <i>region</i> .fms
	com.amazonaws. <i>region</i> .fms-fips
Amazon Forecast	com.amazonaws. <i>region</i> .prakiraan
	com.amazonaws. <i>region</i> .kueri prakiraan
	com.amazonaws. <i>region</i> .ramalan-fips

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .forecastquery-fips
Detektor Penipuan Amazon	com.amazonaws. <i>region</i> .detektor penipuan
Amazon FSx	com.amazonaws. <i>region</i> .fsx
	com.amazonaws. <i>region</i> .fsx-fips
GameLift Server Amazon	com.amazonaws. <i>region</i> .gamelift
Aliran GameLift Amazon	com.amazonaws. <i>region</i> .gameliftstream
AWS Global Networks for Transit Gateways	com.amazonaws. <i>region</i> .pengelola jaringan
AWS Glue	com.amazonaws. <i>region</i> .lem
	com.amazonaws. <i>region</i> .glu.dasbor
AWS Glue DataBrew	com.amazonaws. <i>region</i> .database
	com.amazonaws. <i>region</i> .databrew-fips
Amazon Managed Grafana	com.amazonaws. <i>region</i> .grafana
	com.amazonaws. <i>region</i> .grafana-ruang kerja
AWS Ground Station	com.amazonaws. <i>region</i> .stasiun bawah tanah
	com.amazonaws. <i>region</i> .groundstation-fips
Amazon GuardDuty	com.amazonaws. <i>region</i> .tugas penjaga
	com.amazonaws. <i>region</i> .guardduty-data
	com.amazonaws. <i>region</i> .guardduty-data-fips
	com.amazonaws. <i>region</i> .guardduty-fips
AWS HealthImaging	com.amazonaws. <i>region</i> .dicom-medis-pencitraan

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .pencitraan medis
	com.amazonaws. <i>region</i> .pencitraan medis runtime-
AWS HealthLake	com.amazonaws. <i>region</i> .danau kesehatan
AWS HealthOmics	com.amazonaws. <i>region</i> .analitik-omik
	com.amazonaws. <i>region</i> .analitik-omics-fips
	com.amazonaws. <i>region</i> .control-storage-omics
	com.amazonaws. <i>region</i> .control-penyimpanan-omics-fips
	com.amazonaws. <i>region</i> .storage-omics
	com.amazonaws. <i>region</i> .tag-omics
	com.amazonaws. <i>region</i> .tag-omics-fips
	com.amazonaws. <i>region</i> .alur kerja-omik
	com.amazonaws. <i>region</i> .alur kerja-omics-fips
AWS Identity and Access Management (IAM)	com.amazonaws.iam
Penganalisis Akses IAM	com.amazonaws. <i>region</i> .access-penganalisis
	com.amazonaws. <i>region</i> .access-analiser-fips
Pusat Identitas IAM	com.amazonaws. <i>region</i> .toko identitas
	com.amazonaws. <i>region</i> .sso
	com.amazonaws. <i>region</i> .sso-oauth
IAM Roles Anywhere	com.amazonaws. <i>region</i> .roldi mana saja

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .rolesanywhere-fips
Amazon Inspector	com.amazonaws. <i>region</i> .inspektor2
	com.amazonaws. <i>region</i> .inspektor2-fips
	com.amazonaws. <i>region</i> .inspektor-pindai
	com.amazonaws. <i>region</i> .inspektor-scan-fips
Amazon Interactive Video Service	com.amazonaws. <i>region</i> .ivs.berkontribusi
AWS IoT Core	com.amazonaws. <i>region</i> .iot.api
	com.amazonaws. <i>region</i> .iot-fips.api
	com.amazonaws. <i>region</i> .iot.data
	com.amazonaws. <i>region</i> .iot.kredensial
AWS IoT Device Management terowongan aman	com.amazonaws. <i>region</i> .iot.tunneling.api
	com.amazonaws. <i>region</i> .iot-fips.tuneling.api
	com.amazonaws. <i>region</i> .iot. Tunnel.data
	com.amazonaws. <i>region</i> .iot-fips.tunel.data
AWS IoT Core Device Advisor	com.amazonaws. <i>region</i> .perangkat.iot
Integrasi terkelola untuk AWS IoT Device Management	com.amazonaws. <i>region</i> .iotmanagedintegrations.api
	com.amazonaws. <i>region</i> .iotmanagedintegrasi-fips.api
AWS IoT Core for LoRaWAN	com.amazonaws. <i>region</i> .iotwireless.api
	com.amazonaws. <i>region</i> .lorawan.cups
	com.amazonaws. <i>region</i> .lorawan.lns

Layanan AWS	Nama layanan
AWS IoT FleetWise	com.amazonaws. <i>region</i> .iotfleetwise
AWS IoT Greengrass	com.amazonaws. <i>region</i> .rumput hijau
AWS IoT RoboRunner	com.amazonaws. <i>region</i> .iotroborunner
AWS IoT SiteWise	com.amazonaws. <i>region</i> .iotsitewise.api
	com.amazonaws. <i>region</i> .iotsitewise.data
AWS IoT TwinMaker	com.amazonaws. <i>region</i> .iottwinmaker.api
	com.amazonaws. <i>region</i> .iottwinmaker.data
Amazon Kendra	com.amazonaws. <i>region</i> .kendra
	aws.api. <i>region</i> .kendra-peringkat
AWS Key Management Service	com.amazonaws. <i>region</i> .km
	com.amazonaws. <i>region</i> .kms-fips
Amazon Keyspaces (untuk Apache Cassandra)	com.amazonaws. <i>region</i> .cassandra
	com.amazonaws. <i>region</i> .cassandra-fips
Aliran Data Amazon Kinesis	com.amazonaws. <i>region</i> .kinesis-aliran
	com.amazonaws. <i>region</i> .kinesis-streams-fips
AWS Lake Formation	com.amazonaws. <i>region</i> .formasi danau
AWS Lambda	com.amazonaws. <i>region</i> .lambda
	com.amazonaws. <i>region</i> .lambda-microvm
AWS Launch Wizard	com.amazonaws. <i>region</i> .launchwizard
Amazon Lex V2	com.amazonaws. <i>region</i> .model-v2-lex

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .runtime-v2-lex
AWS License Manager	com.amazonaws. <i>region</i> .pengelola lisensi
	com.amazonaws. <i>region</i> .lisensi-manager-fips
	com.amazonaws. <i>region</i> .license-manager-langgan-linux
	com.amazonaws. <i>region</i> .lisensi-manager-linux-langgan-fips
	com.amazonaws. <i>region</i> .lisensi-manager-pengguna-langgan
	com.amazonaws. <i>region</i> .lisensi-manager-pengguna-langgan-fips
Amazon Lightsail	com.amazonaws. <i>region</i> .light sail
Amazon Location Service	com.amazonaws. <i>region</i> .geo.peta
	com.amazonaws. <i>region</i> .geo.tempat
	com.amazonaws. <i>region</i> .geo.route
	com.amazonaws. <i>region</i> .geo.geofencing
	com.amazonaws. <i>region</i> .geo.tracking
	com.amazonaws. <i>region</i> .geo.metadata
Amazon Lookout untuk Peralatan	com.amazonaws. <i>region</i> .lookoutperlengkapan
Amazon Lookout untuk Visi	com.amazonaws. <i>region</i> .lookoutvision
Amazon Macie	com.amazonaws. <i>region</i> .macie2
	com.amazonaws. <i>region</i> .macie2-fips

Layanan AWS	Nama layanan
AWS Mainframe Modernization	com.amazonaws. <i>region</i> .tes aplikasi
	com.amazonaws. <i>region</i> .m2
Amazon Managed Blockchain	com.amazonaws. <i>region</i> .managedblockchain-query
	com.amazonaws. <i>region</i> .managedblockchain.bitcoin.mainnet
	com.amazonaws. <i>region</i> .managedblockchain.bitcoin.testnet
AWS Perjanjian Pasar	com.amazonaws. <i>region</i> .perjanjian-pasar
AWS Penemuan Pasar	com.amazonaws. <i>region</i> .penemuan-pasar
AWS Marketplace Metering Service	com.amazonaws. <i>region</i> .meter-pasar
Layanan Terkelola Amazon untuk Prometheus	com.amazonaws. <i>region</i> .aps
	com.amazonaws. <i>region</i> .aps-ruang kerja
Streaming Terkelola Amazon untuk Apache Kafka (MSK)	com.amazonaws. <i>region</i> .kafka
	com.amazonaws. <i>region</i> .kafka-fips
Alur Kerja Terkelola Amazon untuk Apache Airflow	com.amazonaws. <i>region</i> .airflow.api
	com.amazonaws. <i>region</i> .airflow.api-fips
	com.amazonaws. <i>region</i> .airflow.env
	com.amazonaws. <i>region</i> .airflow.env-fips
	com.amazonaws. <i>region</i> .airflow.ops
Amazon Route 53	com.amazonaws.route53
Amazon Route 53 Global Resolver	aws.api.us-east-2.route53globalresolver

Layanan AWS	Nama layanan
	aws.api.us-east-2.route53globalresolver-fips
Profil Amazon Route 53	com.amazonaws. <i>region</i> .route53profil
Konsol Manajemen AWS	com.amazonaws. <i>region</i> .konsol
	com.amazonaws. <i>region</i> .login
Memori AmazonDB	com.amazonaws. <i>region</i> .memory-db
	com.amazonaws. <i>region</i> .memorydb-fips
Orkestrator AWS Migration Hub	com.amazonaws. <i>region</i> .migrationhub orkestrator
AWS Migration Hub Refactor Spaces	com.amazonaws. <i>region</i> .refactor-spasi
Rekomendasi Strategi Pusat Migrasi	com.amazonaws. <i>region</i> .migrationhub-strategi
Amazon MQ	com.amazonaws. <i>region</i> .mq
	com.amazonaws. <i>region</i> .mq-fips
Analisis Amazon Neptune	com.amazonaws. <i>region</i> .neptune-graf
	com.amazonaws. <i>region</i> .neptune-graf-data
	com.amazonaws. <i>region</i> .neptune-graph-fips
AWS Network Firewall	com.amazonaws. <i>region</i> .network-firewall
	com.amazonaws. <i>region</i> .network-firewall-fips
OpenSearch Layanan Amazon	Titik akhir ini dikelola layanan
Konsumsi OpenSearch Amazon	com.amazonaws. <i>region</i> .osis
AWS Organizations	com.amazonaws. <i>region</i> .organisasi
	com.amazonaws. <i>region</i> .organisasi-fips

Layanan AWS	Nama layanan
AWS Outposts	com.amazonaws. <i>region</i> .pos terdepan
AWS Panorama	com.amazonaws. <i>region</i> .panorama
AWS Kriptografi Pembayaran	com.amazonaws. <i>region</i> .pembayaran-kriptografi.con trolplane
	com.amazonaws. <i>region</i> .pembayaran-kriptografi.dat aplane
AWS PCS	com.amazonaws. <i>region</i> .pcs
	com.amazonaws. <i>region</i> .pcs-fips
Personalisasi Amazon	com.amazonaws. <i>region</i> .personalisasi
	com.amazonaws. <i>region</i> .personalisasi-acara
	com.amazonaws. <i>region</i> .personalisasi-runtime
Titik Pintu Amazon	com.amazonaws. <i>region</i> .menunjukkan
	com.amazonaws. <i>region</i> .pinpoint-sms-suara-v2
Amazon Polly	com.amazonaws. <i>region</i> .polly
	com.amazonaws. <i>region</i> .polly-fips
Daftar Harga AWS	com.amazonaws. <i>region</i> .harga.api
AWS Private Certificate Authority	com.amazonaws. <i>region</i> .acm-pca
	com.amazonaws. <i>region</i> .acm-pca-fips
	com.amazonaws. <i>region</i> .pca-connector-iklan
	com.amazonaws. <i>region</i> .pca-connector-scep
AWS Proton	com.amazonaws. <i>region</i> .proton

Layanan AWS	Nama layanan
Bisnis Amazon Q	aws.api. <i>region</i> .qbisnis
Amazon Q Developer	com.amazonaws. <i>region</i> .codewhisperer
	com.amazonaws. <i>region</i> .q
	com.amazonaws. <i>region</i> .qapps
Langganan Pengguna Amazon Q	com.amazonaws. <i>region</i> .layanan.pengguna-langganan
Quick	com.amazonaws. <i>region</i> .quicksight situs web
Amazon RDS	com.amazonaws. <i>region</i> .rds
	com.amazonaws. <i>region</i> .rds-fips
API Data Amazon RDS	com.amazonaws. <i>region</i> .rds-data
Wawasan Performa Amazon RDS	com.amazonaws. <i>region</i> .pi
	com.amazonaws. <i>region</i> .pi-fips
AWS Re: Post Pribadi	com.amazonaws. <i>region</i> .repostspace
Keranjang Sampah	com.amazonaws. <i>region</i> .rbin
	com.amazonaws. <i>region</i> .rbin-fips
Amazon Redshift	com.amazonaws. <i>region</i> .pergeseran merah
	com.amazonaws. <i>region</i> .redshift-fips
	com.amazonaws. <i>region</i> .redshift-tanpa server
	com.amazonaws. <i>region</i> .redshift-serverless-fips
API Data Pergeseran Merah Amazon	com.amazonaws. <i>region</i> .redshift-data
	com.amazonaws. <i>region</i> .redshift-data-fips

Layanan AWS	Nama layanan
Amazon Recognition	com.amazonaws. <i>region</i> .Recognition
	com.amazonaws. <i>region</i> .Recognition-fips
	com.amazonaws. <i>region</i> .streaming Recognition
	com.amazonaws. <i>region</i> .streaming-recognition-fips
AWS Resource Access Manager	com.amazonaws. <i>region</i> .ram
	com.amazonaws. <i>region</i> .ram-fips
Penjelajah Sumber Daya AWS	com.amazonaws. <i>region</i> .sumber daya-explorer-2
	com.amazonaws. <i>region</i> .resource-explorer-2-fips
AWS Resource Groups	com.amazonaws. <i>region</i> .kelompok sumber daya
	com.amazonaws. <i>region</i> .sumber daya-grup-fips
AWS Resource Groups Tagging API	com.amazonaws. <i>region</i> .penandaan
Amazon S3	com.amazonaws. <i>region</i> .s3
	com.amazonaws. <i>region</i> .s3-fips
	com.amazonaws. <i>region</i> .s3tabel
Titik Ak Multi-Region ses Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws. <i>region</i> .s3-pos terdepan
Amazon SageMaker AI	aws.pembuat saji. <i>region</i> .eksperimen
	aws.pembuat saji. <i>region</i> .buku catatan
	aws.pembuat saji. <i>region</i> .partner-app
	aws.pembuat saji. <i>region</i> .studio

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .sagemaker-data-sains-asisten
	com.amazonaws. <i>region</i> .sagemaker.api
	com.amazonaws. <i>region</i> .sagemaker.api-fips
	com.amazonaws. <i>region</i> .sagemaker.featurestore-run time
	com.amazonaws. <i>region</i> .sagemaker.featurestore-run time-fips
	com.amazonaws. <i>region</i> .sagemaker.metrics
	com.amazonaws. <i>region</i> .sagemaker.runtime
	com.amazonaws. <i>region</i> .sagemaker.runtime-fips
Paket Tabungan	com.amazonaws.savingsplans
AWS Secrets Manager	com.amazonaws. <i>region</i> .manajer rahasia
AWS Agen Keamanan	com.amazonaws. <i>region</i> .agen keamanan
AWS Security Hub CSPM	com.amazonaws. <i>region</i> .pusat keamanan
	com.amazonaws. <i>region</i> .securityhub-fips
Amazon Security Lake	com.amazonaws. <i>region</i> .sekuriti
	com.amazonaws. <i>region</i> .securitylake-fips
AWS Security Token Service	com.amazonaws. <i>region</i> .sts
	com.amazonaws. <i>region</i> .sts-fips
AWS Serverless Application Repository	com.amazonaws. <i>region</i> .serverlessrepo

Layanan AWS	Nama layanan
Service Catalog	com.amazonaws. <i>region</i> .katalog layanan
	com.amazonaws. <i>region</i> .servicecatalog-appregistry
Kuota Layanan	com.amazonaws. <i>region</i> .service Quotes
Amazon SES	com.amazonaws. <i>region</i> .email-smtp
	com.amazonaws. <i>region</i> .mail-manager
	com.amazonaws. <i>region</i> .mail-manager-fips
	com.amazonaws. <i>region</i> .mail-manager-smtp.auth.fips
	com.amazonaws. <i>region</i> .mail-manager-smtp.open.fips
AWS Snowball Edge Device Management	com.amazonaws. <i>region</i> .manajemen perangkat-salju
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> .sqs
	com.amazonaws. <i>region</i> .sqs-fips
Amazon SWF	com.amazonaws. <i>region</i> .swf
	com.amazonaws. <i>region</i> .swf-fips
AWS Step Functions	com.amazonaws. <i>region</i> .negara
	com.amazonaws. <i>region</i> .sinkronisasi status
AWS Storage Gateway	com.amazonaws. <i>region</i> .cara penyimpanan
Rantai Pasokan AWS	com.amazonaws. <i>region</i> .scn
AWS Systems Manager	com.amazonaws. <i>region</i> .ec2pesan
	com.amazonaws. <i>region</i> .ssm

Layanan AWS	Nama layanan
	com.amazonaws. <i>region</i> .ssm-kontak
	com.amazonaws. <i>region</i> .ssm-insiden
	com.amazonaws. <i>region</i> .ssm-insidan-fips
	com.amazonaws. <i>region</i> .ssm-pengaturan cepat
	com.amazonaws. <i>region</i> .sms pesan
Manajer Sistem AWS untuk SAP	com.amazonaws. <i>region</i> .ssm-sap
	com.amazonaws. <i>region</i> .ssm-sap-fips
AWS Pembangun Jaringan Telco	com.amazonaws. <i>region</i> .tnb
Amazon Textract	com.amazonaws. <i>region</i> .teks
	com.amazonaws. <i>region</i> .textract-fips
Amazon Timestream	com.amazonaws. <i>region</i> .timestream.ingest- <i>cell</i>
	com.amazonaws. <i>region</i> .timestream.query- <i>cell</i>
Amazon Timestream untuk InfluxDB	com.amazonaws. <i>region</i> .timestream-influxdb
	com.amazonaws. <i>region</i> .timestream-influxdb-fips
Transkrip Amazon	com.amazonaws. <i>region</i> .transkripsikan
	com.amazonaws. <i>region</i> .transkripsi-fips
	com.amazonaws. <i>region</i> .transskripsistreaming
com.amazonaws. <i>region</i> .transcribestreaming-fips	
Amazon Transkrip Medis	com.amazonaws. <i>region</i> .transkripsikan
	com.amazonaws. <i>region</i> .transskripsistreaming

Layanan AWS	Nama layanan
AWS Transfer Family	com.amazonaws. <i>region</i> .transfer
AWS Transform	com.amazonaws. <i>region</i> .transformasi
AWS Transform adat	com.amazonaws. <i>region</i> .transform-kustom
Terjemahkan Amazon	com.amazonaws. <i>region</i> .menerjemahkan
AWS Trusted Advisor	com.amazonaws. <i>region</i> .penasihat terpercaya
Notifikasi Pengguna AWS	com.amazonaws. <i>region</i> .notifikasi
	com.amazonaws. <i>region</i> .notifikasi-kontak
Izin Terverifikasi Amazon	com.amazonaws. <i>region</i> .izin terverifikasi
	com.amazonaws. <i>region</i> .izin terverifikasi-fips
Amazon VPC Lattice	com.amazonaws. <i>region</i> .vpc-latex
AWS WAFV2	com.amazonaws. <i>region</i> .wafv2
	com.amazonaws. <i>region</i> .wafv2 fips
AWS Well-Architected Tool	com.amazonaws. <i>region</i> .didesain dengan baik
Amazon WorkMail	com.amazonaws. <i>region</i> .email kerja
	com.amazonaws. <i>region</i> .workmailaliran pesan
Amazon WorkSpaces	com.amazonaws. <i>region</i> .ruang kerja
Peram WorkSpaces ban Aman Amazon	com.amazonaws. <i>region</i> .ruang kerja-web
	com.amazonaws. <i>region</i> .ruang kerja-web-fips
WorkSpaces streaming	com.amazonaws. <i>region</i> .dataran tinggi
Klien WorkSpaces Tipis Amazon	com.amazonaws. <i>region</i> .thinclient.api

Layanan AWS	Nama layanan
aws.api. <i>region</i> .s3file	
aws.api. <i>region</i> .s3files-fips	
AWS X-Ray	com.amazonaws. <i>region</i> .xray
Layanan Terkelola Amazon untuk Apache Flink	com.amazonaws. <i>region</i> .kinesisanalitik
	com.amazonaws. <i>region</i> .kinesisanalytics-fips

Lihat tersedia Layanan AWS nama

Anda dapat menggunakan [perintah](#) `describe-vpc-endpoint-services` untuk melihat nama layanan yang mendukung titik akhir VPC.

Contoh berikut menampilkan titik akhir antarmuka Layanan AWS yang mendukung di Wilayah yang ditentukan. `--query Opsi` membatasi output ke nama layanan.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

```
[
  "api.aws.us-east-1.cassandra-streams",
  "aws.api.us-east-1.bcm-data-exports",
  "aws.api.us-east-1.emr-service-cell01",
  "aws.api.us-east-1.freetier",
  "aws.api.us-east-1.kendra-ranking",
  "aws.api.us-east-1.qbusiness",
  . . .
  "com.amazonaws.us-east-1.xray"
]
```

Melihat informasi tentang layanan

Setelah Anda memiliki nama layanan, Anda dapat menggunakan [perintah](#) `describe-vpc-endpoint-services` untuk melihat informasi terperinci tentang setiap layanan titik akhir.

Contoh berikut menampilkan informasi tentang titik akhir CloudWatch antarmuka Amazon di Wilayah yang ditentukan.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

Berikut ini adalah contoh output. `VpcEndpointPolicySupported` menunjukkan apakah [kebijakan titik akhir](#) didukung. `SupportedIpAddressTypes` menunjukkan jenis alamat IP mana yang didukung.

```
{
  "ServiceDetails": [
    {
      "ServiceName": "com.amazonaws.us-east-1.monitoring",
      "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
      "ServiceType": [
        {
          "ServiceType": "Interface"
        }
      ],
      "AvailabilityZones": [
        "us-east-1a",
        "us-east-1b",
        "us-east-1c",
        "us-east-1d",
        "us-east-1e",
        "us-east-1f"
      ],
      "Owner": "amazon",
      "BaseEndpointDnsNames": [
        "monitoring.us-east-1.vpce.amazonaws.com"
      ],
      "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
      "PrivateDnsNames": [
        {
          "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
        }
      ]
    }
  ]
}
```

```

    },
    {
      "PrivateDnsName": "monitoring.us-east-1.api.aws"
    },
    {
      "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
    },
    {
      "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
    }
  ],
  "VpcEndpointPolicySupported": true,
  "AcceptanceRequired": false,
  "ManagesVpcEndpoints": false,
  "Tags": [],
  "PrivateDnsNameVerificationState": "verified",
  "SupportedIpAddressTypes": [
    "ipv6",
    "ipv4"
  ]
},
{
  "ServiceNames": [
    "com.amazonaws.us-east-1.monitoring"
  ]
}
}

```

Lihat dukungan kebijakan titik akhir

Untuk memverifikasi apakah layanan mendukung kebijakan [titik akhir](#), panggil [perintah](#) `describe-vpc-endpoint-services` dan periksa nilainya. `VpcEndpointPolicySupported` Nilai yang mungkin adalah `true` dan `false`.

Contoh berikut memeriksa apakah layanan yang ditentukan mendukung kebijakan titik akhir di Wilayah yang ditentukan. `--query` Opsi membatasi output ke nilai `VpcEndpointPolicySupported`.

```

aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text

```

Berikut ini adalah output contoh.

```
True
```

Contoh berikut mencantumkan kebijakan titik akhir Layanan AWS yang mendukung di Wilayah yang ditentukan. `--queryOpsi` membatasi output ke nama layanan. Untuk menjalankan perintah ini menggunakan command prompt Windows, hapus tanda kutip tunggal di sekitar string kueri, dan ubah karakter kelanjutan baris dari `\` menjadi `^`.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

```
[
  "api.aws.us-east-1.cassandra-streams",
  "aws.api.us-east-1.bcm-data-exports",
  "aws.api.us-east-1.emr-service-cell01",
  "aws.api.us-east-1.freetier",
  "aws.api.us-east-1.kendra-ranking",
  . . .
  "com.amazonaws.us-east-1.xray"
]
```

Contoh berikut mencantumkan kebijakan titik akhir Layanan AWS yang tidak mendukung di Wilayah yang ditentukan. `--queryOpsi` membatasi output ke nama layanan. Untuk menjalankan perintah ini menggunakan command prompt Windows, hapus tanda kutip tunggal di sekitar string kueri, dan ubah karakter kelanjutan baris dari `\` menjadi `^`.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

```
[
```

```

    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    . . .
]

```

Lihat dukungan IPv6

Untuk melihat dukungan IPv6 untuk AWS layanan, lihat [AWS layanan yang mendukung IP v6](#). Anda juga dapat menggunakan [perintah](#) `describe-vpc-endpoint-services` berikut untuk melihat yang dapat Anda akses melalui IPv6 di Wilayah Layanan AWS yang ditentukan. `--queryOps` membatasi output ke nama layanan.

```

aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
  Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames

```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

```

[
  "api.aws.us-east-1.cassandra-streams",
  "aws.api.us-east-1.bcm-data-exports",
  "aws.api.us-east-1.freetier",
  "aws.api.us-east-1.kendra-ranking",
  "aws.api.us-east-1.qbusiness",
  "aws.api.us-east-1.resource-explorer-2",
  "aws.api.us-east-1.resource-explorer-2-fips",
  "aws.sagemaker.us-east-1.experiments",
  "aws.sagemaker.us-east-1.partner-app",
  "com.amazonaws.iam",
  "com.amazonaws.us-east-1.access-analyzer",
  "com.amazonaws.us-east-1.account",
  . . .
  "com.amazonaws.us-east-1.xray"
]

```

Cross-region diaktifkan Layanan AWS

Berikut ini Layanan AWS terintegrasi dengan lintas wilayah AWS PrivateLink. Anda dapat membuat titik akhir antarmuka untuk terhubung ke layanan ini di Wil AWS ayah lain, secara pribadi, seolah-olah mereka berjalan di VPC Anda sendiri.

Pilih tautan di Layanan AWS kolom untuk melihat dokumentasi layanan. Kolom Nama layanan berisi nama layanan yang Anda tentukan saat membuat titik akhir antarmuka.

Layanan AWS	Nama layanan
Amazon S3	com.amazonaws. <i>region</i> .s3
AWS Identity and Access Management (IAM)	com.amazonaws.iam
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
AWS Key Management Service	com.amazonaws. <i>region</i> .km
	com.amazonaws. <i>region</i> .kms-fips
Amazon ECS	com.amazonaws. <i>region</i> .ecs
AWS Lambda	com.amazonaws. <i>region</i> .lambda
Selang Api Data Amazon	com.amazonaws. <i>region</i> .kinesis-firehose
Layanan Terkelola Amazon untuk Apache Flink	com.amazonaws. <i>region</i> .kinesisanalitik
	com.amazonaws. <i>region</i> .kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Lihat tersedia Layanan AWS nama

Anda dapat menggunakan [perintah](#) describe-vpc-endpoint-services untuk melihat layanan yang diaktifkan lintas Wilayah.

Contoh berikut menampilkan Layanan AWS bahwa pengguna di Wil us-east-1 ayah dapat mengakses melalui titik akhir antarmuka, ke Wilayah layanan (us-west-2) yang ditentukan. --query Opsi membatasi output ke nama layanan.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

```
[
  "com.amazonaws.us-west-2.ecr.api",
  "com.amazonaws.us-west-2.ecr.dkr",
  "com.amazonaws.us-west-2.ecs",
  "com.amazonaws.us-west-2.ecs-fips",
  ...
  "com.amazonaws.us-west-2.s3"
]
```

Note

Anda harus menggunakan DNS regional. DNS Zonal tidak didukung saat mengakses Layanan AWS di Wilayah lain. Untuk informasi selengkapnya, [lihat Melihat dan memperbarui atribut DNS](#) di Panduan Pengguna Amazon VPC.

Izin dan Pertimbangan

- Secara default, entitas IAM tidak memiliki izin untuk mengakses Layanan AWS di Wilayah lain. Untuk memberikan izin yang diperlukan untuk akses lintas Wilayah, administrator IAM dapat membuat kebijakan IAM yang mengizinkan tindakan khusus `izinvpce:AllowMultiRegion`.
- Pastikan Kebijakan Kontrol Layanan (SCP) Anda tidak menolak tindakan khusus `vpce:AllowMultiRegion` izin. Untuk menggunakan AWS PrivateLink fitur konektivitas lintas wilayah, kebijakan identitas dan SCP Anda harus mengizinkan tindakan ini.
- Untuk mengontrol Wilayah yang entitas IAM dapat menentukan sebagai Wilayah layanan saat membuat titik akhir VPC, gunakan kunci `ec2:VpceServiceRegion` kondisi.

- Konsumen layanan harus memilih Wilayah opt-in sebelum memilihnya sebagai Wilayah layanan untuk titik akhir. Jika memungkinkan, kami menyarankan agar konsumen layanan mengakses layanan menggunakan konektivitas intra-wilayah alih-alih konektivitas lintas wilayah. Intra-Region konektivitas memberikan latensi yang lebih rendah dan biaya yang lebih rendah.
- Anda dapat menggunakan kunci kondisi aws :SourceVpcArn global baru IAM untuk mengamankan Wilayah, Akun AWS dan VPC mana sumber daya Anda dapat diakses. Kunci ini membantu menerapkan residensi data dan kontrol akses berbasis wilayah.
- Untuk ketersediaan tinggi, buat titik akhir antarmuka yang diaktifkan lintas Wilayah di setidaknya dua Zona Ketersediaan. Dalam hal ini, penyedia dan konsumen tidak diharuskan menggunakan Zona Ketersediaan yang sama.
- Dengan akses lintas Wilayah, AWS PrivateLink mengelola failover antara Zona Ketersediaan di Wilayah layanan dan konsumen. Itu tidak mengelola failover di seluruh Wilayah.
- Akses Lintas Wilayah tidak didukung untuk Zona Ketersediaan berikut: use1-az3usw1-az2,apne1-az3,,apne2-az2, danapne2-az4.
- Anda dapat menggunakan AWS Fault Injection Service untuk mensimulasikan peristiwa regional dan skenario kegagalan model untuk titik akhir antarmuka yang diaktifkan dalam wilayah dan lintas wilayah. Untuk mempelajari lebih lanjut, lihat [AWS FIS dokumentasi](#).

Membuat titik akhir antarmuka ke Layanan AWS di daerah lain

Untuk membuat titik akhir antarmuka menggunakan Konsol, lihat [bagian](#) Membuat titik akhir VPC.

Di CLI, Anda dapat menggunakan [perintah](#) `create-vpc-endpoint` untuk membuat titik akhir VPC ke wilayah yang berbeda. Layanan AWS Contoh berikut membuat titik akhir antarmuka ke Amazon S3 us-west-2 dari VPC dius-east-1.

```
aws ec2 create-vpc-endpoint \  
  --vpc-id vpc-id \  
  --service-name com.amazonaws.us-west-2.s3 \  
  --vpc-endpoint-type Interface \  
  --subnet-ids subnet-id-1 subnet-id-2 \  
  --region us-east-1 \  
  --service-region us-west-2
```

Akses Layanan AWS menggunakan antarmuka titik akhir VPC

Anda dapat membuat antarmuka titik akhir VPC untuk terhubung ke layanan yang didukung AWS PrivateLink, termasuk banyak Layanan AWS. Untuk ikhtisar, lihat [the section called “Konsep”](#) dan [Akses Layanan AWS](#).

Untuk setiap subnet yang Anda tentukan dari VPC Anda, kami membuat antarmuka jaringan titik akhir di subnet dan menetapkan alamat IP pribadi dari rentang alamat subnet. Antarmuka jaringan titik akhir adalah antarmuka jaringan yang dikelola permintaan; Anda dapat melihatnya di Akun AWS, tetapi Anda tidak dapat mengelolanya sendiri.

Anda ditagih untuk biaya penggunaan dan pemrosesan data per jam. Untuk informasi selengkapnya, lihat [Harga titik akhir antarmuka](#).

Daftar Isi

- [Prasyarat](#)
- [Buat VPC endpoint](#)
- [Subnet bersama](#)
- [ICMP](#)

Prasyarat

- Menyebarkan sumber daya yang akan mengakses Layanan AWS di VPC Anda.
- Untuk menggunakan DNS pribadi, Anda harus mengaktifkan nama host DNS dan resolusi DNS untuk VPC Anda. Untuk informasi selengkapnya, [lihat Melihat dan memperbarui atribut DNS](#) di Panduan Pengguna Amazon VPC.
- Untuk mengaktifkan IPv6 untuk titik akhir antarmuka, Layanan AWS harus mendukung akses melalui IPv6. Untuk informasi selengkapnya, lihat [the section called “Jenis alamat IP”](#).
- Buat grup keamanan untuk antarmuka jaringan titik akhir yang memungkinkan lalu lintas yang diharapkan dari sumber daya di VPC Anda. Misalnya, untuk memastikan bahwa AWS CLI dapat mengirim permintaan HTTPS ke Layanan AWS, grup keamanan harus mengizinkan lalu lintas HTTPS masuk.
- Jika sumber daya Anda berada di subnet dengan ACL jaringan, verifikasi bahwa ACL jaringan memungkinkan lalu lintas antara sumber daya di VPC Anda dan antarmuka jaringan titik akhir.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat [AWS PrivateLink kuota](#).

Buat VPC endpoint

Gunakan prosedur berikut untuk membuat titik akhir VPC antarmuka yang terhubung ke Layanan AWS

Untuk membuat titik akhir antarmuka untuk Layanan AWS

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih AWS layanan.
5. (Opsional) Jika membuat titik akhir ke Layanan AWS wilayah lain, pilih kotak centang Aktifkan titik akhir lintas wilayah lalu pilih wilayah layanan dari drop-down.
6. Untuk Nama layanan, pilih layanan. Untuk informasi selengkapnya, lihat [the section called “Layanan yang terintegrasi”](#).
7. Untuk VPC, pilih VPC dari mana Anda akan mengakses Layanan AWS
8. Jika, pada Langkah 5, Anda memilih nama layanan untuk Amazon S3, dan jika Anda ingin mengonfigurasi dukungan DNS [pribadi](#), pilih Pengaturan tambahan, Aktifkan nama DNS. Ketika Anda membuat pilihan ini, itu juga secara otomatis memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk. Anda dapat mengonfigurasi DNS pribadi dengan titik akhir Resolver masuk hanya untuk titik akhir antarmuka untuk Amazon S3. Jika Anda tidak memiliki titik akhir gateway untuk Amazon S3 dan memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk, Anda akan menerima kesalahan saat mencoba langkah terakhir dalam prosedur ini.

Jika, pada Langkah 5, Anda memilih nama layanan untuk layanan apa pun selain Amazon S3, Pengaturan tambahan, Aktifkan nama DNS sudah dipilih. Kami menyarankan Anda mempertahankan default. Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik akhir VPC Anda.

9. Untuk Subnet, pilih subnet tempat untuk membuat antarmuka jaringan titik akhir. Anda dapat memilih satu subnet per Zona Ketersediaan. Anda tidak dapat memilih beberapa subnet dari Zona Ketersediaan yang sama. Untuk informasi selengkapnya, lihat [the section called “Subnet dan Zona Ketersediaan”](#).

Secara default, kami memilih alamat IP dari rentang alamat IP subnet dan menetapkan ke antarmuka jaringan titik akhir. Untuk memilih alamat IP sendiri, pilih Tetapkan alamat IP.

Perhatikan bahwa empat alamat IP pertama dan alamat IP terakhir dalam blok CIDR subnet dicadangkan untuk penggunaan internal, sehingga Anda tidak dapat menentukannya untuk antarmuka jaringan titik akhir Anda.

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

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

11. Untuk grup keamanan, pilih grup keamanan yang akan diasosiasikan dengan antarmuka jaringan titik akhir. Secara default, kami mengaitkan grup keamanan default untuk VPC.

12. Untuk Kebijakan, untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya melalui titik akhir antarmuka, pilih Akses penuh. Untuk membatasi akses, pilih Kustom dan masukkan kebijakan. Opsi ini hanya tersedia jika layanan mendukung kebijakan titik akhir VPC. Untuk informasi selengkapnya, lihat [Kebijakan titik akhir](#).

13. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.

14. Pilih Buat titik akhir.

Untuk membuat titik akhir antarmuka menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Titik akhir VPC yang dikelola oleh AWS layanan (titik akhir VPC yang dikelola layanan) dapat dibuat oleh layanan di subnet bersama.

ICMP

Titik akhir antarmuka tidak menanggapi ping permintaan. Anda dapat menggunakan `nc` atau sebagai gantinya.

Konfigurasi titik akhir antarmuka

Setelah Anda membuat antarmuka VPC endpoint, Anda dapat memperbarui konfigurasinya.

Tugas

- [Menambah atau menghapus subnet](#)
- [Grup keamanan asosiasi](#)
- [Edit kebijakan titik akhir VPC](#)
- [Aktifkan nama DNS pribadi](#)
- [Kelola tanda](#)

Menambah atau menghapus subnet

Anda dapat memilih satu subnet per Availability Zone untuk titik akhir antarmuka Anda. Jika Anda menambahkan subnet, kami membuat antarmuka jaringan endpoint di subnet dan menetapkan alamat IP pribadi dari rentang alamat IP subnet. Jika Anda menghapus subnet, kami menghapus antarmuka jaringan endpoint-nya. Untuk informasi selengkapnya, lihat [the section called “Subnet dan Zona Ketersediaan”](#).

Untuk mengubah subnet menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola subnet.
5. Pilih atau batal pilihan Availability Zones sesuai kebutuhan. Untuk setiap Availability Zone, pilih satu subnet. Secara default, kami memilih alamat IP dari rentang alamat IP subnet dan menetapkan ke antarmuka jaringan titik akhir. Untuk memilih alamat IP untuk antarmuka jaringan titik akhir, pilih Tentukan alamat IP dan masukkan alamat IPv4 dari rentang alamat

subnet. Jika layanan endpoint mendukung IPv6, Anda juga dapat memasukkan alamat IPv6 dari rentang alamat subnet.

Jika Anda menentukan alamat IP untuk subnet yang sudah memiliki antarmuka jaringan endpoint untuk titik akhir VPC ini, kami mengganti antarmuka jaringan endpoint dengan yang baru. Proses ini untuk sementara memutuskan subnet dan titik akhir VPC.

6. Pilih Ubah subnet.

Untuk mengubah subnet menggunakan baris perintah

- [memodifikasi-vpc-titik akhir \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

Grup keamanan asosiasi

Anda dapat mengubah grup keamanan yang terkait dengan antarmuka jaringan untuk titik akhir antarmuka Anda. Aturan grup keamanan mengontrol lalu lintas yang diizinkan ke antarmuka jaringan titik akhir dari sumber daya di VPC Anda.

Untuk mengubah grup keamanan menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola grup keamanan.
5. Pilih atau batalkan pilihan grup keamanan sesuai kebutuhan.
6. Pilih Ubah grup keamanan.

Untuk mengubah grup keamanan menggunakan baris perintah

- [memodifikasi-vpc-titik akhir \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

Edit kebijakan titik akhir VPC

Jika Layanan AWS mendukung kebijakan titik akhir, Anda dapat mengedit kebijakan titik akhir untuk titik akhir. Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan. Untuk informasi selengkapnya, lihat [Kebijakan titik akhir](#).

Untuk mengubah kebijakan titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan kustom.
6. Pilih Simpan.

Untuk mengubah kebijakan endpoint menggunakan baris perintah

- [memodifikasi-vpc-titik akhir](#) ()AWS CLI
- [Edit-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Aktifkan nama DNS pribadi

Kami menyarankan Anda mengaktifkan nama DNS pribadi untuk titik akhir VPC Anda. Layanan AWS ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik akhir VPC Anda.

Untuk menggunakan nama DNS pribadi, Anda harus mengaktifkan [nama host DNS dan resolusi DNS untuk VPC](#) Anda. Setelah Anda mengaktifkan nama DNS pribadi, mungkin diperlukan beberapa menit agar alamat IP pribadi tersedia. Catatan DNS yang kami buat saat Anda mengaktifkan nama DNS pribadi bersifat pribadi. Oleh karena itu, nama DNS pribadi tidak dapat diselesaikan secara publik.

Untuk mengubah opsi nama DNS pribadi menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>

2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Ubah nama DNS pribadi.
5. Pilih atau hapus Aktifkan untuk titik akhir ini sesuai kebutuhan.
6. Jika layanannya Amazon S3, memilih Aktifkan untuk titik akhir ini di langkah sebelumnya juga memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk. Jika Anda lebih suka fungsi DNS pribadi standar, hapus Aktifkan DNS pribadi hanya untuk titik akhir masuk. Jika Anda tidak memiliki titik akhir gateway untuk Amazon S3 selain titik akhir antarmuka untuk Amazon S3, dan Anda memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk, Anda akan menerima kesalahan saat menyimpan perubahan di langkah berikutnya. Untuk informasi selengkapnya, lihat [the section called “DNS privat”](#).
7. Pilih Simpan perubahan.

Untuk mengubah opsi nama DNS pribadi menggunakan baris perintah

- [memodifikasi-vpc-titik akhir](#) ()AWS CLI
- [Edit-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Kelola tanda

Anda dapat menandai titik akhir antarmuka Anda untuk membantu Anda mengidentifikasi atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk mengelola tag menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag untuk menambahkan pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag menggunakan baris perintah

- [buat-tag dan hapus-tag](#) ()AWS CLI
- [New-EC2Tag](#) dan [Remove-EC2Tag](#) (Alat untuk Windows PowerShell)

Menerima peringatan untuk peristiwa titik akhir antarmuka

Anda dapat membuat notifikasi untuk menerima peringatan untuk peristiwa tertentu yang terkait dengan titik akhir antarmuka Anda. Misalnya, Anda dapat menerima email ketika permintaan koneksi diterima atau ditolak.

Tugas

- [Buat notifikasi SNS](#)
- [Menambahkan kebijakan akses](#)
- [Menambahkan kebijakan utama](#)

Buat notifikasi SNS

Gunakan prosedur berikut untuk membuat topik Amazon SNS untuk notifikasi dan berlangganan topik tersebut.

Untuk membuat notifikasi untuk titik akhir antarmuka menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Dari tab Notifikasi, pilih Buat notifikasi.
5. Untuk Notifikasi ARN, pilih Nama Sumber Daya [Amazon](#) (ARN) untuk topik SNS yang Anda buat.
6. Untuk berlangganan acara, pilih dari A cara.
 - Hu bungkan — Konsumen layanan membuat titik akhir antarmuka. Ini mengirimkan permintaan koneksi ke penyedia layanan.
 - Terima — Penyedia layanan menerima permintaan koneksi.
 - Tol ak — Penyedia layanan menolak permintaan koneksi.

- Hapus — Konsumen layanan menghapus titik akhir antarmuka.

7. Pilih Buat notifikasi.

Untuk membuat notifikasi untuk titik akhir antarmuka menggunakan baris perintah

- [buat-notifikasi sambungan titik-akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpointConnectionNotification](#)(Alat untuk Windows PowerShell)

Menambahkan kebijakan akses

Tambahkan kebijakan akses ke topik Amazon SNS yang memungkinkan AWS PrivateLink untuk mempublikasikan pemberitahuan atas nama Anda, seperti berikut ini. Untuk informasi selengkapnya, lihat [Bagaimana cara mengedit kebijakan akses topik Amazon SNS saya?](#) Gunakan kunci kondisi `aws:SourceArn` dan `aws:SourceAccount` global untuk melindungi dari masalah wakil yang [membingungkan](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "111111111111"
        }
      }
    }
  ]
}
```

```
}
```

Menambahkan kebijakan utama

Jika Anda menggunakan topik SNS terenkripsi, kebijakan sumber daya untuk kunci KMS harus dipercaya untuk memanggil AWS PrivateLink operasi AWS KMS API. Berikut ini adalah contoh kebijakan utama.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "111111111111"
        }
      }
    }
  ]
}
```

Menghapus titik akhir antarmuka

Setelah selesai dengan titik akhir VPC, Anda dapat menghapusnya. Menghapus titik akhir antarmuka juga menghapus antarmuka jaringan titik akhir.

Untuk menghapus titik akhir antarmuka menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir antarmuka menggunakan baris perintah

- [hapus titik akhir vpc \(\)](#) AWS CLI
- [Remove-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Titik akhir Gateway

Titik akhir Gateway VPC menyediakan konektivitas yang andal ke Amazon S3 dan DynamoDB tanpa memerlukan gateway internet atau perangkat NAT untuk VPC Anda. Titik akhir gateway tidak digunakan AWS PrivateLink, tidak seperti jenis titik akhir VPC lainnya.

Amazon S3 dan DynamoDB mendukung titik akhir gateway dan titik akhir antarmuka. Untuk perbandingan opsi, lihat yang berikut ini:

- [Jenis titik akhir VPC untuk Amazon S3](#)
- [Jenis titik akhir VPC untuk Amazon DynamoDB](#)

Harga

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

Daftar Isi

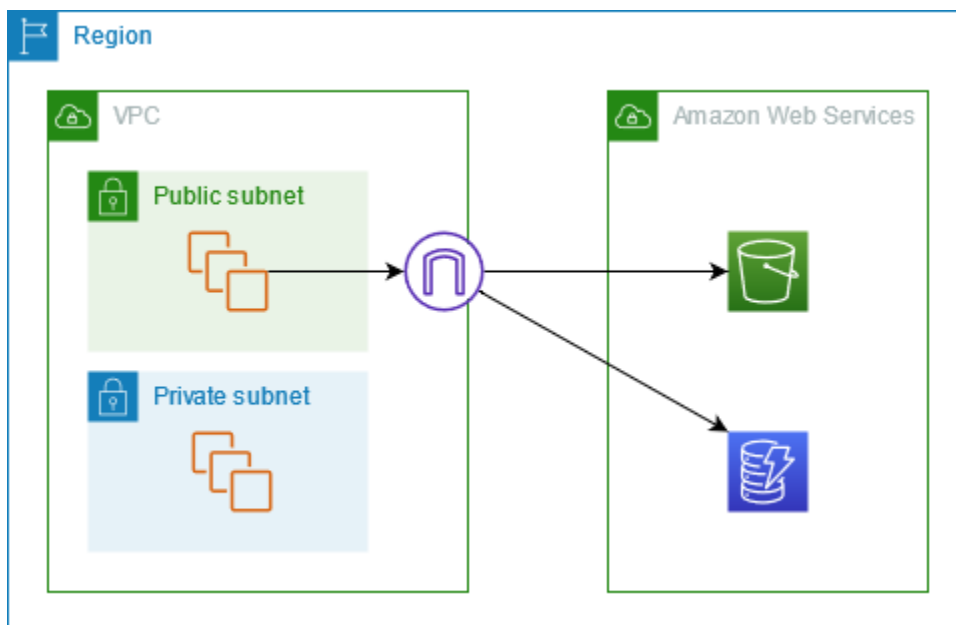
- [Gambaran umum](#)
- [Perutean](#)
- [Keamanan](#)
- [Jenis alamat IP](#)
- [Jenis IP catatan DNS](#)
- [Titik akhir gateway untuk Amazon S3](#)
- [Titik akhir gateway untuk Amazon DynamoDB](#)

Gambaran umum

Anda dapat mengakses Amazon S3 dan DynamoDB melalui titik akhir layanan publik mereka atau melalui titik akhir gateway. Ikhtisar ini membandingkan metode ini.

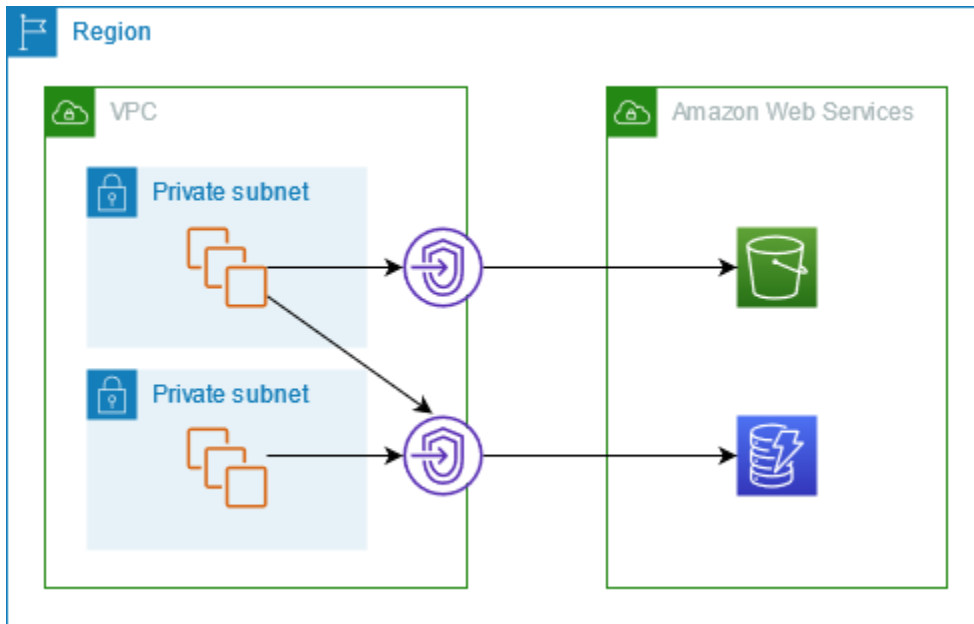
Akses melalui gateway internet

Diagram berikut menunjukkan bagaimana instans mengakses Amazon S3 dan DynamoDB melalui titik akhir layanan publik mereka. Lalu lintas ke Amazon S3 atau DynamoDB dari instance di subnet publik dialihkan ke gateway internet untuk VPC dan kemudian ke layanan. Instans di subnet pribadi tidak dapat mengirim lalu lintas ke Amazon S3 atau DynamoDB, karena menurut definisi subnet pribadi tidak memiliki rute ke gateway internet. Untuk mengaktifkan instance di subnet pribadi untuk mengirim lalu lintas ke Amazon S3 atau DynamoDB, Anda harus menambahkan perangkat NAT ke subnet publik dan merutekan lalu lintas di subnet pribadi ke perangkat NAT. Sementara lalu lintas ke Amazon S3 atau DynamoDB melintasi gateway internet, itu tidak meninggalkan jaringan. AWS



Akses melalui titik akhir gateway

Diagram berikut menunjukkan bagaimana instans mengakses Amazon S3 dan DynamoDB melalui titik akhir gateway. Lalu lintas dari VPC Anda ke Amazon S3 atau DynamoDB dialihkan ke titik akhir gateway. Setiap tabel rute subnet harus memiliki rute yang mengirimkan lalu lintas yang ditujukan untuk layanan ke titik akhir gateway menggunakan daftar awalan untuk layanan. Untuk informasi selengkapnya, lihat [AWS daftar awalan yang dikelola](#) di Panduan Pengguna Amazon VPC.



Perutean

Saat Anda membuat titik akhir gateway, Anda memilih tabel rute VPC untuk subnet yang Anda aktifkan. Rute berikut secara otomatis ditambahkan ke setiap tabel rute yang Anda pilih. Tujuan adalah daftar awalan untuk layanan yang dimiliki oleh AWS dan targetnya adalah titik akhir gateway.

Tujuan	Target
<i>prefix_list_id</i>	<i>gateway_endpoint_id</i>

Pertimbangan-pertimbangan

- Anda dapat meninjau rute titik akhir yang kami tambahkan ke tabel rute, tetapi Anda tidak dapat mengubah atau menghapusnya. Untuk menambahkan rute titik akhir ke tabel rute, kaitkan dengan titik akhir gateway. Kami menghapus rute titik akhir saat Anda memisahkan tabel rute dari titik akhir gateway atau ketika Anda menghapus titik akhir gateway.

- Semua instance di subnet yang terkait dengan tabel rute yang terkait dengan titik akhir gateway secara otomatis menggunakan titik akhir gateway untuk mengakses layanan. Instans di subnet yang tidak terkait dengan tabel rute ini menggunakan titik akhir layanan publik, bukan titik akhir gateway.
- Tabel rute dapat memiliki rute titik akhir ke Amazon S3 dan rute titik akhir ke DynamoDB. Anda dapat memiliki rute titik akhir ke layanan yang sama (Amazon S3 atau DynamoDB) di beberapa tabel rute. Anda tidak dapat memiliki beberapa rute titik akhir ke layanan yang sama (Amazon S3 atau DynamoDB) dalam satu tabel rute.
- Kami menggunakan rute paling spesifik yang cocok dengan lalu lintas untuk menentukan cara merutekan lalu lintas (kecocokan awalan terpanjang). Untuk tabel rute dengan rute titik akhir, ini berarti sebagai berikut:
 - Jika ada rute yang mengirimkan semua lalu lintas internet (0.0.0. 0/0) ke gateway internet, rute titik akhir diutamakan untuk lalu lintas yang ditujukan untuk layanan (Amazon S3 atau DynamoDB) di Wilayah saat ini. Lalu lintas yang ditujukan untuk Layanan AWS penggunaan yang berbeda dari gateway internet.
 - Lalu lintas yang ditujukan untuk layanan (Amazon S3 atau DynamoDB) di Wilayah yang berbeda masuk ke gateway internet karena daftar awalan khusus untuk Wilayah.
 - Jika ada rute yang menentukan rentang alamat IP yang tepat untuk layanan (Amazon S3 atau DynamoDB) di Wilayah yang sama, rute tersebut diutamakan daripada rute titik akhir.

Keamanan

Saat instans Anda mengakses Amazon S3 atau DynamoDB melalui titik akhir gateway, instans mengakses layanan menggunakan titik akhir publiknya. Grup keamanan untuk instans ini harus mengizinkan lalu lintas ke dan dari layanan. Berikut ini adalah contoh aturan keluar. Ini mereferensikan ID [daftar awalan](#) untuk layanan.

Tujuan	Protokol	Rentang port
<i>prefix_list_id</i>	TCP	443

ACL jaringan untuk subnet untuk instans ini juga harus mengizinkan lalu lintas ke dan dari layanan. Berikut ini adalah contoh aturan keluar. Anda tidak dapat mereferensikan daftar awalan dalam aturan ACL jaringan, tetapi Anda bisa mendapatkan rentang alamat IP untuk layanan dari daftar awalannya.

Tujuan	Protokol	Rentang port
<i>service_cidr_block_1</i>	TCP	443
<i>service_cidr_block_2</i>	TCP	443
<i>service_cidr_block_3</i>	TCP	443

Jenis alamat IP

Jenis alamat IP menentukan daftar awalan mana yang terkait dengan tabel rute Anda.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir gateway

- Jenis alamat IP dari titik akhir gateway harus kompatibel dengan subnet untuk titik akhir gateway, seperti yang dijelaskan di sini:
 - IPv4 — Tambahkan daftar awalan IPv4 layanan ke tabel rute Anda.
 - IPv6 — Tambahkan daftar awalan IPv6 layanan ke tabel rute Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
 - Dualstack — Tambahkan daftar awalan IPv4 layanan ke tabel rute Anda dan tambahkan daftar awalan IPv6 layanan ke tabel rute Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

Jenis IP catatan DNS

Secara default, titik akhir gateway mengembalikan catatan DNS berdasarkan titik akhir layanan yang Anda panggil. Jika Anda membuat titik akhir gateway menggunakan titik akhir layanan IPv4, seperti `seperti3.us-east-2.amazonaws.com`, Amazon S3 mengembalikan catatan A ke klien Anda, dan semua subnet di tabel rute Anda menggunakan IPv4.

Sebaliknya, jika Anda membuat titik akhir gateway menggunakan titik akhir layanan dualstack, seperti `seperti3.dualstack.us-east-2.amazonaws.com`, Amazon S3 mengembalikan catatan A dan AAAA ke klien Anda, dan subnet di tabel rute Anda menggunakan IPv4 dan IPv6.

Note

Untuk bucket direktori, atau S3 Express One Zone, titik akhir gateway untuk bidang data akan menjadi `s3express-use2-az1.us-east-2.amazonaws.com` dan `s3express-use2-az1.dualstack.us-east-2.amazonaws.com` masing-masing.

Jenis IP catatan DNS memengaruhi cara lalu lintas dialihkan ke klien Anda. Jika Anda membuat titik akhir gateway menggunakan titik akhir layanan IPv4 dan kemudian memanggil titik akhir layanan dualstack, lalu lintas yang menggunakan catatan AAAA tidak akan dialihkan melalui titik akhir gateway. Lalu lintas akan dijatuhkan atau dialihkan IPv6-compatible melalui jalur jika ada. Jika Anda menggunakan jenis IP catatan DNS yang ditentukan layanan, pastikan layanan Anda dapat menangani panggilan variabel dari beberapa titik akhir layanan.

Alih-alih pengaturan tipe IP catatan DNS default dari layanan [yang ditentukan](#), Anda dapat menyesuaikan jenis IP catatan DNS untuk memilih rekaman mana yang dikembalikan untuk titik akhir tertentu. Tabel berikut menunjukkan jenis IP catatan DNS yang didukung dan jenis rekaman yang dikembalikan:

Jenis IP catatan DNS	Jenis rekaman yang dikembalikan
IPv4	A
IPv6	AAAA
Tumpukan ganda	A dan AAAA
layanan yang ditentukan	Catatan tergantung pada titik akhir layanan

Untuk memilih jenis IP catatan DNS, Anda harus menggunakan jenis alamat IP yang kompatibel untuk layanan titik akhir. Tabel berikut menunjukkan jenis IP catatan DNS yang didukung untuk setiap jenis alamat IP untuk titik akhir gateway:

Jenis alamat IP	Jenis IP catatan DNS yang didukung
IPv4	IPv4, layanan yang ditentukan layanan*
IPv6	IPv6, layanan yang ditentukan layanan*

Jenis alamat IP	Jenis IP catatan DNS yang didukung
Dualstack	IPv4, IPv6, Dualstack, layanan yang ditentukan layanan*

* Merupakan tipe IP catatan DNS default.

Note

Untuk menggunakan tipe IP rekaman DNS selain yang ditentukan layanan untuk titik akhir Gateway, Anda harus mengizinkan `enableDnsSupport` dan `enableDnsHostnames` atribut dalam pengaturan VPC Anda.

Anda tidak dapat mengubah tipe IP catatan DNS untuk titik akhir gateway DynamoDB. DynamoDB hanya mendukung jenis IP record DNS dari layanan yang ditentukan.

Perilaku tipe IP catatan DNS berbeda untuk titik akhir antarmuka. Untuk informasi selengkapnya, lihat [Jenis IP catatan DNS untuk titik akhir antarmuka](#).

Titik akhir gateway untuk Amazon S3

Anda dapat mengakses Amazon S3 dari VPC menggunakan titik akhir VPC gateway. Setelah membuat titik akhir gateway, Anda dapat menambahkannya sebagai target di tabel rute untuk lalu lintas yang ditujukan dari VPC ke Amazon S3.

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

Amazon S3 mendukung titik akhir gateway dan titik akhir antarmuka. Dengan titik akhir gateway, Anda dapat mengakses Amazon S3 dari VPC Anda, tanpa memerlukan gateway internet atau perangkat NAT untuk VPC Anda, dan tanpa biaya tambahan. Namun, titik akhir gateway tidak mengizinkan akses dari jaringan lokal, dari VPC yang diintip di Wil AWS ayah lain, atau melalui gateway transit. Untuk skenario tersebut, Anda harus menggunakan titik akhir antarmuka, yang tersedia dengan biaya tambahan. Untuk informasi selengkapnya, lihat [Jenis titik akhir VPC untuk Amazon S3](#) di Panduan Pengguna Amazon S3.

Daftar Isi

- [Pertimbangan-pertimbangan](#)

- [DNS privat](#)
- [Buat titik akhir gateway](#)
- [Kontrol akses menggunakan kebijakan bucket](#)
- [Asosiasikan tabel rute](#)
- [Mengedit kebijakan titik akhir VPC](#)
- [Menghapus titik akhir gateway](#)

Pertimbangan-pertimbangan

- Titik akhir gateway hanya tersedia di Wilayah tempat Anda membuatnya. Pastikan untuk membuat titik akhir gateway Anda di Wilayah yang sama dengan bucket S3 Anda.
- Jika Anda menggunakan server DNS Amazon, Anda harus mengaktifkan nama host [DNS dan resolusi DNS](#) untuk VPC Anda. Jika Anda menggunakan server DNS Anda sendiri, pastikan permintaan ke Amazon S3 diselesaikan dengan benar ke alamat IP yang dikelola oleh AWS.
- Aturan untuk grup keamanan untuk instans Anda yang mengakses Amazon S3 melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari Amazon S3. Anda dapat mereferensikan ID [daftar awalan](#) untuk Amazon S3 dalam aturan grup keamanan.
- ACL jaringan untuk subnet untuk instans Anda yang mengakses Amazon S3 melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari Amazon S3. Anda tidak dapat mereferensikan daftar awalan dalam aturan ACL jaringan, tetapi Anda bisa mendapatkan rentang alamat IP untuk Amazon S3 dari daftar [awalan](#) untuk Amazon S3.
- Periksa apakah Anda menggunakan Layanan AWS yang memerlukan akses ke bucket S3. Misalnya, layanan mungkin memerlukan akses ke bucket yang berisi file log, atau mungkin mengharuskan Anda mengunduh driver atau agen ke instans EC2 Anda. Jika demikian, pastikan kebijakan titik akhir Anda mengizinkan sumber daya Layanan AWS atau mengakses bucket ini menggunakan `s3:GetObject` tindakan tersebut.
- Anda tidak dapat menggunakan `aws:SourceIp` kondisi dalam kebijakan identitas atau kebijakan bucket untuk permintaan ke Amazon S3 yang melintasi titik akhir VPC. Sebagai gantinya, gunakan `aws:VpcSourceIp` kondisi tersebut. Atau, Anda dapat menggunakan tabel rute untuk mengontrol instans EC2 mana yang dapat mengakses Amazon S3 melalui titik akhir VPC.
- Alamat IPv4 atau IPv6 sumber dari instance di subnet yang terpengaruh seperti yang diterima oleh Amazon S3 berubah dari alamat publik menjadi alamat pribadi di VPC Anda. Titik akhir mengalihkan rute jaringan, dan memutuskan koneksi TCP terbuka. Koneksi sebelumnya yang menggunakan alamat publik tidak dilanjutkan. Sebaiknya Anda tidak menjalankan tugas penting

apa pun saat Anda membuat atau memodifikasi titik akhir; atau Anda menguji untuk memastikan bahwa perangkat lunak Anda dapat terhubung kembali secara otomatis ke Amazon S3 setelah koneksi terputus.

- Koneksi titik akhir tidak dapat diperpanjang dari VPC. Sumber daya di sisi lain koneksi VPN, koneksi peering VPC, gateway transit, atau Direct Connect koneksi di VPC Anda tidak dapat menggunakan titik akhir gateway untuk berkomunikasi dengan Amazon S3.
- Akun Anda memiliki kuota default 20 titik akhir gateway per Wilayah, yang dapat disesuaikan. Ada juga batas 255 titik akhir gateway per VPC.

DNS privat

Anda dapat mengonfigurasi DNS pribadi untuk mengoptimalkan biaya saat membuat titik akhir gateway dan titik akhir antarmuka untuk Amazon S3.

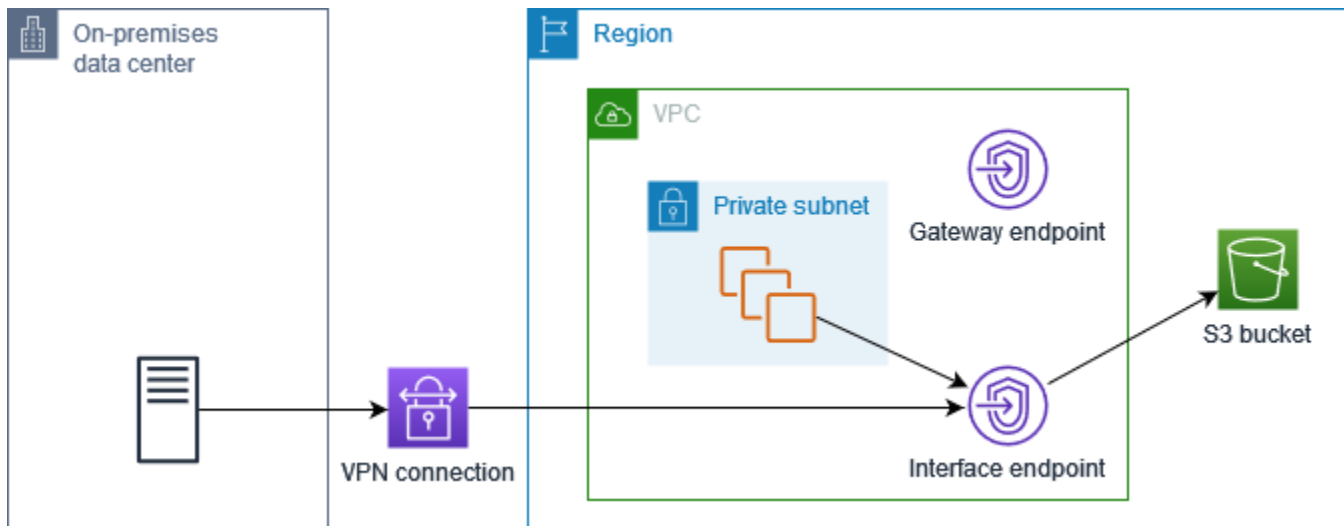
Route 53 Resolver

Amazon menyediakan server DNS, yang disebut [Route 53 Resolver](#), untuk VPC Anda. Route 53 Resolver secara otomatis menyelesaikan nama domain VPC lokal dan catatan di zona pribadi yang dihosting. Namun, Anda tidak dapat menggunakan Route 53 Resolver dari luar VPC Anda. Route 53 menyediakan titik akhir Resolver dan aturan Resolver sehingga Anda dapat menggunakan Route 53 Resolver dari luar VPC Anda. Titik akhir Resolver masuk meneruskan kueri DNS dari jaringan lokal ke Route 53 Resolver. Titik akhir Resolver keluar meneruskan kueri DNS dari Route 53 Resolver ke jaringan lokal.

Saat Anda mengonfigurasi titik akhir antarmuka untuk Amazon S3 agar menggunakan DNS pribadi hanya untuk titik akhir Resolver masuk, kami membuat titik akhir Resolver masuk. Titik akhir Resolver masuk menyelesaikan kueri DNS ke Amazon S3 dari lokal ke alamat IP pribadi dari titik akhir antarmuka. Kami juga menambahkan catatan ALIAS untuk Route 53 Resolver ke zona yang dihosting publik untuk Amazon S3, sehingga kueri DNS dari VPC Anda diselesaikan ke alamat IP publik Amazon S3, yang merutekan lalu lintas ke titik akhir gateway.

DNS privat

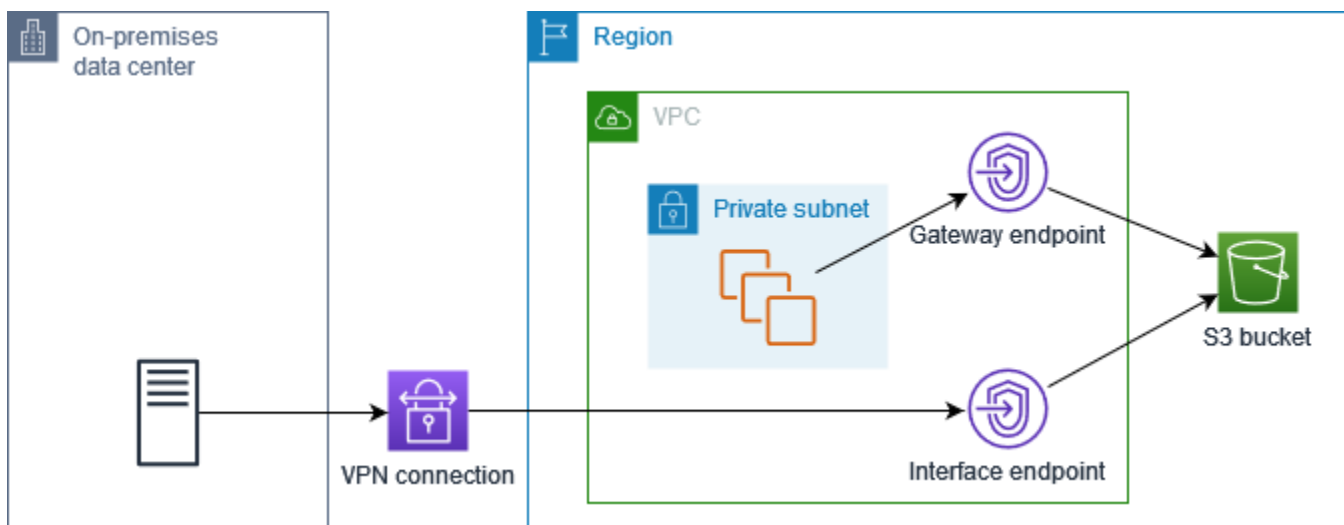
Jika Anda mengonfigurasi DNS pribadi untuk titik akhir antarmuka untuk Amazon S3 tetapi tidak mengonfigurasi DNS pribadi hanya untuk titik akhir Resolver masuk, permintaan dari jaringan lokal dan VPC Anda menggunakan titik akhir antarmuka untuk mengakses Amazon S3. Oleh karena itu, Anda membayar untuk menggunakan titik akhir antarmuka untuk lalu lintas dari VPC, alih-alih menggunakan titik akhir gateway tanpa biaya tambahan.



DNS pribadi hanya untuk titik akhir Resolver masuk

Jika Anda mengonfigurasi DNS pribadi hanya untuk titik akhir Resolver masuk, permintaan dari jaringan lokal Anda menggunakan titik akhir antarmuka untuk mengakses Amazon S3, dan permintaan dari VPC Anda menggunakan titik akhir gateway untuk mengakses Amazon S3. Oleh karena itu, Anda mengoptimalkan biaya Anda, karena Anda membayar untuk menggunakan titik akhir antarmuka hanya untuk lalu lintas yang tidak dapat menggunakan titik akhir gateway.

Untuk mengonfigurasi ini, tipe IP catatan DNS dari titik akhir gateway harus sesuai dengan titik akhir antarmuka atau `beservice-defined`. AWS PrivateLink tidak mendukung kombinasi lainnya. Untuk informasi selengkapnya, lihat [the section called “Jenis IP catatan DNS”](#).



Konfigurasi DNS pribadi

Anda dapat mengonfigurasi DNS pribadi untuk titik akhir antarmuka untuk Amazon S3 saat Anda membuatnya atau setelah Anda membuatnya. Untuk informasi selengkapnya, lihat [the section called “Buat VPC endpoint”](#) (konfigurasi selama pembuatan) atau [the section called “Aktifkan nama DNS pribadi”](#) (konfigurasi setelah pembuatan).

Buat titik akhir gateway

Gunakan prosedur berikut untuk membuat titik akhir gateway yang terhubung ke Amazon S3.

Untuk membuat titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Kategori layanan, pilih Layanan AWS.
5. Untuk Layanan, tambahkan filter Type = Gateway.

Jika data Amazon S3 Anda disimpan dalam bucket tujuan umum, pilih `com.amazonaws.
region.3`.

Jika data Amazon S3 Anda disimpan dalam bucket direktori, pilih `com.amazonaws.
region.s3ekspress`.

6. Untuk VPC, pilih VPC tempat membuat titik akhir.
7. Untuk jenis alamat IP, pilih dari opsi berikut:
 - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan layanan menerima permintaan IPv4.
 - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6 dan layanan menerima permintaan IPv6.
 - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6 dan layanan menerima permintaan IPv4 dan IPv6.
8. Untuk Tabel rute, pilih tabel rute yang akan digunakan oleh titik akhir. Kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir.

9. Untuk Kebijakan, pilih **Ak ses penuh** untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya melalui titik akhir VPC. Jika tidak, pilih **Kustom** untuk melampirkan kebijakan titik akhir VPC yang mengontrol izin yang dimiliki kepala sekolah untuk melakukan tindakan pada sumber daya melalui titik akhir VPC.
10. (Opsional) Untuk menambahkan tanda, pilih **Tambahkan tanda baru** dan masukkan kunci dan nilai tanda.
11. Pilih **Buat titik akhir**.

Untuk membuat titik akhir gateway menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

Kontrol akses menggunakan kebijakan bucket

Anda dapat menggunakan kebijakan bucket untuk mengontrol akses ke bucket dari titik akhir tertentu, VPC, rentang alamat IP, dan. Akun AWS Contoh-contoh ini mengasumsikan bahwa ada juga pernyataan kebijakan yang memungkinkan akses yang diperlukan untuk kasus penggunaan Anda.

Example Contoh: Batasi akses ke titik akhir tertentu

Anda dapat membuat kebijakan bucket yang membatasi akses ke titik akhir tertentu dengan menggunakan kunci kondisi [AWS:source](#) VPCE. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali titik akhir gateway yang ditentukan digunakan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui Konsol Manajemen AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
```

```

        "arn:aws:s3:::bucket_name/*"],
    "Condition": {
        "StringNotEquals": {
            "aws:sourceVpce": "vpce-1a2b3c4d"
        }
    }
}
]
}

```

Example Contoh: Batasi akses ke VPC tertentu

Anda dapat membuat kebijakan bucket yang membatasi akses ke VPC tertentu dengan menggunakan kunci kondisi [AWS: sourceVpc](#). Ini berguna jika Anda memiliki beberapa titik akhir yang dikonfigurasi dalam VPC yang sama. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali permintaan berasal dari VPC yang ditentukan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui Konsol Manajemen AWS.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}

```

Example Contoh: Batasi akses ke rentang alamat IP tertentu

Anda dapat membuat kebijakan yang membatasi akses ke rentang alamat IP tertentu dengan menggunakan kunci VpcSourceIp [kondisi](#) aws:. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali permintaan berasal dari alamat IP yang ditentukan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui Konsol Manajemen AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example Contoh: Batasi akses ke bucket di tempat tertentu Akun AWS

Anda dapat membuat kebijakan yang membatasi akses ke bucket S3 di tempat tertentu Akun AWS dengan menggunakan kunci s3:ResourceAccount kondisi. Kebijakan berikut menolak akses ke bucket S3 menggunakan tindakan yang ditentukan kecuali jika dimiliki oleh yang ditentukan Akun AWS.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "Allow-access-to-bucket-in-specific-account",
    "Effect": "Deny",
    "Principal": "*",
    "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
    "Resource": "arn:aws:s3:::*",
    "Condition": {
      "StringNotEquals": {
        "s3:ResourceAccount": "111122223333"
      }
    }
  }
]
}

```

Asosiasikan tabel rute

Anda dapat mengubah tabel rute yang terkait dengan titik akhir gateway. Saat Anda mengaitkan tabel rute, kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir. Saat Anda memisahkan tabel rute, kami secara otomatis menghapus rute titik akhir dari tabel rute.

Untuk mengaitkan tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola tabel rute.
5. Pilih atau batalkan pilihan tabel rute sesuai kebutuhan.
6. Pilih Ubah tabel rute.

Untuk mengaitkan tabel rute menggunakan baris perintah

- [modify-vpc-endpoint \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

Mengedit kebijakan titik akhir VPC

Anda dapat mengedit kebijakan titik akhir untuk titik akhir gateway, yang mengontrol akses ke Amazon S3 dari VPC melalui titik akhir. Setelah Anda memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan. Kebijakan default memungkinkan akses penuh. Untuk informasi selengkapnya, lihat [Kebijakan titik akhir](#).

Untuk mengubah kebijakan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan khusus.
6. Pilih Simpan.

Berikut ini adalah contoh kebijakan titik akhir untuk mengakses Amazon S3.

Example Contoh: Batasi akses ke bucket tertentu

Anda dapat membuat kebijakan yang membatasi akses ke bucket S3 tertentu saja. Ini berguna jika Anda memiliki VPC lain Layanan AWS yang menggunakan bucket S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
```

```

        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
    ]
}
]
}

```

Example Contoh: Membatasi akses ke peran IAM tertentu

Anda dapat membuat kebijakan yang membatasi akses ke peran IAM tertentu. Anda harus menggunakan `aws:PrincipalArn` untuk memberikan akses ke kepala sekolah.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}

```

Example Contoh: Batasi akses ke pengguna di akun tertentu

Anda dapat membuat kebijakan yang membatasi akses ke akun tertentu.

JSON

```

{

```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "Allow-callers-from-specific-account",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalAccount": "111122223333"
      }
    }
  }
]
```

Menghapus titik akhir gateway

Ketika Anda selesai dengan titik akhir gateway, Anda dapat menghapusnya. Saat Anda menghapus titik akhir gateway, kami menghapus rute titik akhir dari tabel rute subnet.

Anda tidak dapat menghapus titik akhir gateway jika DNS pribadi diaktifkan.

Untuk menghapus titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir gateway menggunakan baris perintah

- [hapus titik akhir vpc \(\)](#) AWS CLI
- [Remove-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

Titik akhir gateway untuk Amazon DynamoDB

Anda dapat mengakses Amazon DynamoDB dari VPC menggunakan titik akhir VPC gateway. Setelah Anda membuat titik akhir gateway, Anda dapat menambahkannya sebagai target di tabel rute untuk lalu lintas yang ditujukan dari VPC Anda ke DynamoDB.

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

DynamoDB mendukung titik akhir gateway dan titik akhir antarmuka. Dengan titik akhir gateway, Anda dapat mengakses DynamoDB dari VPC Anda, tanpa memerlukan gateway internet atau perangkat NAT untuk VPC Anda, dan tanpa biaya tambahan. Namun, titik akhir gateway tidak mengizinkan akses dari jaringan lokal, dari VPC yang diintip di Wilayah AWS lain, atau melalui gateway transit. Untuk skenario tersebut, Anda harus menggunakan titik akhir antarmuka, yang tersedia dengan biaya tambahan. Untuk informasi selengkapnya, lihat [Jenis titik akhir VPC untuk DynamoDB](#) di Panduan Pengembang Amazon DynamoDB.

Daftar Isi

- [Pertimbangan-pertimbangan](#)
- [Buat titik akhir gateway](#)
- [Kontrol akses menggunakan kebijakan IAM](#)
- [Asosiasikan tabel rute](#)
- [Mengedit kebijakan titik akhir VPC](#)
- [Menghapus titik akhir gateway](#)

Pertimbangan-pertimbangan

- Titik akhir gateway hanya tersedia di Wilayah tempat Anda membuatnya. Pastikan untuk membuat titik akhir gateway Anda di Wilayah yang sama dengan tabel DynamoDB Anda.
- Jika Anda menggunakan server DNS Amazon, Anda harus mengaktifkan nama host [DNS dan resolusi DNS](#) untuk VPC Anda. Jika Anda menggunakan server DNS Anda sendiri, pastikan permintaan ke DynamoDB diselesaikan dengan benar ke alamat IP yang dikelola oleh AWS.
- Aturan untuk grup keamanan untuk instans Anda yang mengakses DynamoDB melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari DynamoDB. Anda dapat mereferensikan ID daftar [awalan](#) untuk DynamoDB dalam aturan grup keamanan.
- ACL jaringan untuk subnet untuk instans Anda yang mengakses DynamoDB melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari DynamoDB. Anda tidak dapat mereferensikan

daftar awalan dalam aturan ACL jaringan, tetapi Anda bisa mendapatkan rentang alamat IP untuk DynamoDB dari daftar <https://docs.aws.amazon.com/vpc/latest/userguide/working-with-aws-managed-prefix-lists.html> awalan untuk DynamoDB.

- Jika Anda menggunakan AWS CloudTrail untuk mencatat operasi DynamoDB, file log berisi alamat IP pribadi instans EC2 di VPC konsumen layanan dan ID titik akhir gateway untuk setiap permintaan yang dilakukan melalui titik akhir.
- Titik akhir gateway hanya mendukung lalu lintas IPv4.
- Alamat IPv4 sumber dari instance di subnet yang terpengaruh berubah dari alamat IPv4 publik menjadi alamat IPv4 pribadi dari VPC Anda. Titik akhir mengalihkan rute jaringan dan memutuskan koneksi TCP terbuka. Koneksi sebelumnya yang menggunakan alamat IPv4 publik tidak dilanjutkan. Sebaiknya Anda tidak menjalankan tugas penting apa pun saat Anda membuat atau memodifikasi titik akhir gateway. Atau, uji untuk memastikan bahwa perangkat lunak Anda dapat secara otomatis menyambung kembali ke DynamoDB jika koneksi terputus.
- Koneksi titik akhir tidak dapat diperpanjang dari VPC. Sumber daya di sisi lain koneksi VPN, koneksi peering VPC, gateway transit, atau Direct Connect koneksi di VPC Anda tidak dapat menggunakan titik akhir gateway untuk berkomunikasi dengan DynamoDB.
- Akun Anda memiliki kuota default 20 titik akhir gateway per Wilayah, yang dapat disesuaikan. Ada juga batas 255 titik akhir gateway per VPC.

Buat titik akhir gateway

Gunakan prosedur berikut untuk membuat titik akhir gateway yang terhubung ke DynamoDB.

Untuk membuat titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Kategori layanan, pilih Layanan AWS.
5. Untuk Layanan, tambahkan filter Type = Gateway dan pilih `com.amazonaws.
region.dynamodb`.
6. Untuk VPC, pilih VPC tempat membuat titik akhir.
7. Untuk Tabel rute, pilih tabel rute yang akan digunakan oleh titik akhir. Kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir.

8. Untuk Kebijakan, pilih **Akses penuh** untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya melalui titik akhir VPC. Jika tidak, pilih **Kustom** untuk melampirkan kebijakan titik akhir VPC yang mengontrol izin yang dimiliki kepala sekolah untuk melakukan tindakan pada sumber daya melalui titik akhir VPC.
9. (Opsional) Untuk menambahkan tanda, pilih **Tambahkan tanda baru** dan masukkan kunci dan nilai tanda.
10. Pilih **Buat titik akhir**.

Untuk membuat titik akhir gateway menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

Kontrol akses menggunakan kebijakan IAM

Anda dapat membuat kebijakan IAM untuk mengontrol prinsipal IAM mana yang dapat mengakses tabel DynamoDB menggunakan titik akhir VPC tertentu.

Example Contoh: Batasi akses ke titik akhir tertentu

Anda dapat membuat kebijakan yang membatasi akses ke titik akhir VPC tertentu dengan menggunakan kunci kondisi [AWS:SourceVPC](#). Kebijakan berikut menolak akses ke tabel DynamoDB di akun kecuali titik akhir VPC yang ditentukan digunakan. Contoh ini mengasumsikan bahwa ada juga pernyataan kebijakan yang memungkinkan akses yang diperlukan untuk kasus penggunaan Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-from-specific-endpoint",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "dynamodb:*",
      "Resource": "arn:aws:dynamodb:us-east-1:111111111111:table/*",
      "Condition": {
```

```

        "StringNotEquals" : {
            "aws:sourceVpce": "vpce-11aa22bb"
        }
    }
}

```

Example Contoh: Izinkan akses dari peran IAM tertentu

Anda dapat membuat kebijakan yang memungkinkan akses menggunakan peran IAM tertentu. Kebijakan berikut memberikan akses ke peran IAM yang ditentukan.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-from-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}

```

Example Contoh: Memungkinkan akses dari akun tertentu

Anda dapat membuat kebijakan yang hanya mengizinkan akses dari akun tertentu. Kebijakan berikut memberikan akses kepada pengguna di akun yang ditentukan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-from-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Asosiasikan tabel rute

Anda dapat mengubah tabel rute yang terkait dengan titik akhir gateway. Saat Anda mengaitkan tabel rute, kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir. Saat Anda memisahkan tabel rute, kami secara otomatis menghapus rute titik akhir dari tabel rute.

Untuk mengaitkan tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola tabel rute.
5. Pilih atau batalkan pilihan tabel rute sesuai kebutuhan.
6. Pilih Ubah tabel rute.

Untuk mengaitkan tabel rute menggunakan baris perintah

- [modify-vpc-endpoint \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Mengedit kebijakan titik akhir VPC

Anda dapat mengedit kebijakan titik akhir untuk titik akhir gateway, yang mengontrol akses ke DynamoDB dari VPC melalui titik akhir. Setelah Anda memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan. Kebijakan default memungkinkan akses penuh. Untuk informasi selengkapnya, lihat [Kebijakan titik akhir](#).

Untuk mengubah kebijakan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan khusus.
6. Pilih Simpan.

Untuk memodifikasi titik akhir gateway menggunakan baris perintah

- [modify-vpc-endpoint \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Berikut ini adalah contoh kebijakan titik akhir untuk mengakses DynamoDB.

Example Contoh: Izinkan akses baca-saja

Anda dapat membuat kebijakan yang membatasi akses ke akses baca-saja. Kebijakan berikut memberikan izin untuk membuat daftar dan menjelaskan tabel DynamoDB.

```
{
  "Statement": [
    {
```

```

    "Sid": "ReadOnlyAccess",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
    ],
    "Resource": "*"
  }
]
}

```

Example Contoh: Batasi akses ke tabel tertentu

Anda dapat membuat kebijakan yang membatasi akses ke tabel DynamoDB tertentu. Kebijakan berikut memungkinkan akses ke tabel DynamoDB yang ditentukan.

```

{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}

```

Menghapus titik akhir gateway

Ketika Anda selesai dengan titik akhir gateway, Anda dapat menghapusnya. Saat Anda menghapus titik akhir gateway, kami menghapus rute titik akhir dari tabel rute subnet.

Untuk menghapus titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir gateway menggunakan baris perintah

- [hapus titik akhir vpc \(\)](#) AWS CLI
- [Remove-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Akses produk SaaS melalui AWS PrivateLink

Dengan menggunakan AWS PrivateLink, Anda dapat mengakses produk SaaS secara pribadi, seolah-olah mereka berjalan di VPC Anda sendiri.

Daftar Isi

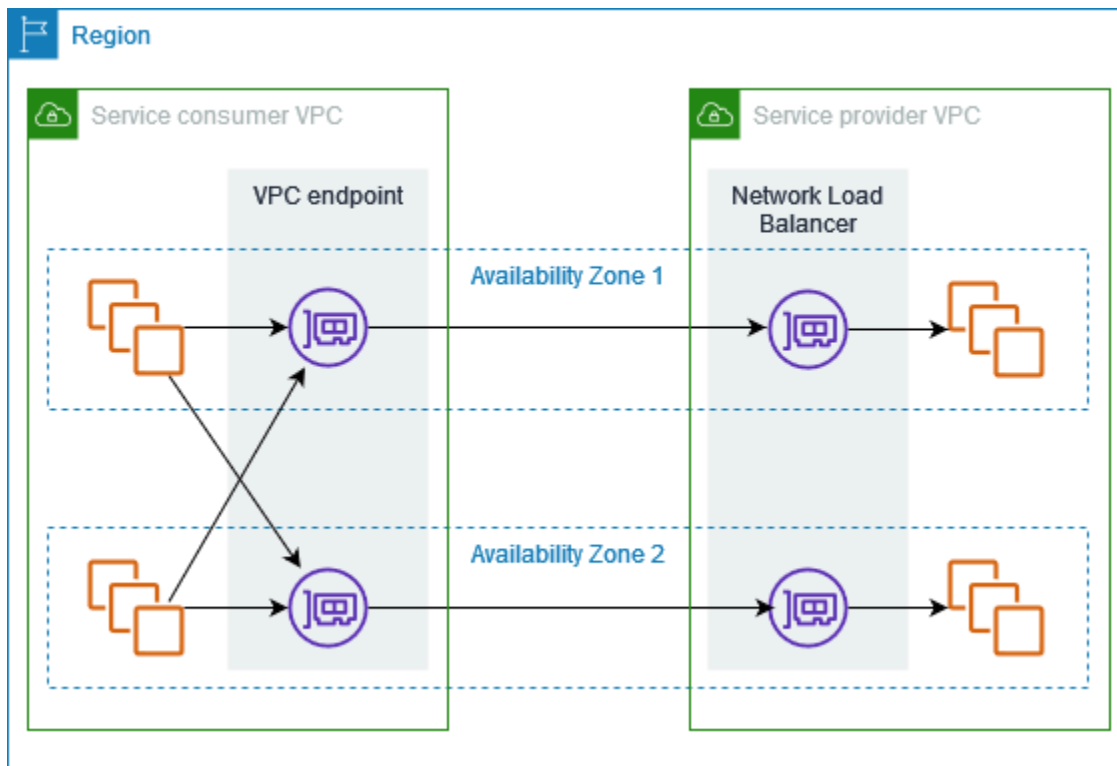
- [Gambaran umum](#)
- [Membuat sebuah titik akhir antarmuka](#)

Gambaran umum

Anda dapat menemukan, membeli, dan menyediakan produk SaaS yang didukung AWS PrivateLink oleh AWS Marketplace. Untuk informasi selengkapnya, lihat [Mengakses aplikasi SaaS dengan aman dan pribadi menggunakan AWS PrivateLink](#).

Anda juga dapat menemukan produk SaaS yang didukung oleh AWS PrivateLink AWS Mitra. Untuk informasi lebih lanjut, lihat [AWS PrivateLink Mitra](#).

Diagram berikut menunjukkan bagaimana Anda menggunakan titik akhir VPC untuk terhubung ke produk SaaS. Penyedia layanan membuat layanan titik akhir dan memberikan pelanggan mereka akses ke layanan titik akhir. Sebagai konsumen layanan, Anda membuat titik akhir VPC antarmuka, yang membuat koneksi antara satu atau lebih subnet di VPC Anda dan layanan titik akhir.



Membuat sebuah titik akhir antarmuka

Gunakan prosedur berikut untuk membuat titik akhir VPC antarmuka yang terhubung ke produk SaaS.

Persyaratan

Berlangganan layanan.

Untuk membuat titik akhir antarmuka ke layanan mitra

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Jika Anda membeli layanan dari AWS Marketplace, lakukan hal berikut:
 - a. Untuk Jenis, pilih AWS Marketplace layanan.
 - b. Pilih layanan.
5. Jika Anda berlangganan layanan dengan penunjukan AWS Service Ready, lakukan hal berikut:

- a. Untuk Jenis, pilih Layanan mitra PrivateLink Siap.
- b. Masukkan nama layanan, lalu pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC dari mana Anda akan mengakses produk.
7. Untuk Subnet, pilih subnet tempat untuk membuat antarmuka jaringan titik akhir.
8. Untuk grup keamanan, pilih grup keamanan yang akan diasosiasikan dengan antarmuka jaringan titik akhir. Aturan grup keamanan harus mengizinkan lalu lintas antara sumber daya di VPC dan antarmuka jaringan titik akhir.
9. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
10. Pilih Buat titik akhir.

Untuk mengonfigurasi titik akhir antarmuka

Untuk informasi tentang mengonfigurasi titik akhir antarmuka Anda, lihat [the section called “Konfigurasi titik akhir antarmuka”](#).

Bagikan layanan Anda melalui AWS PrivateLink

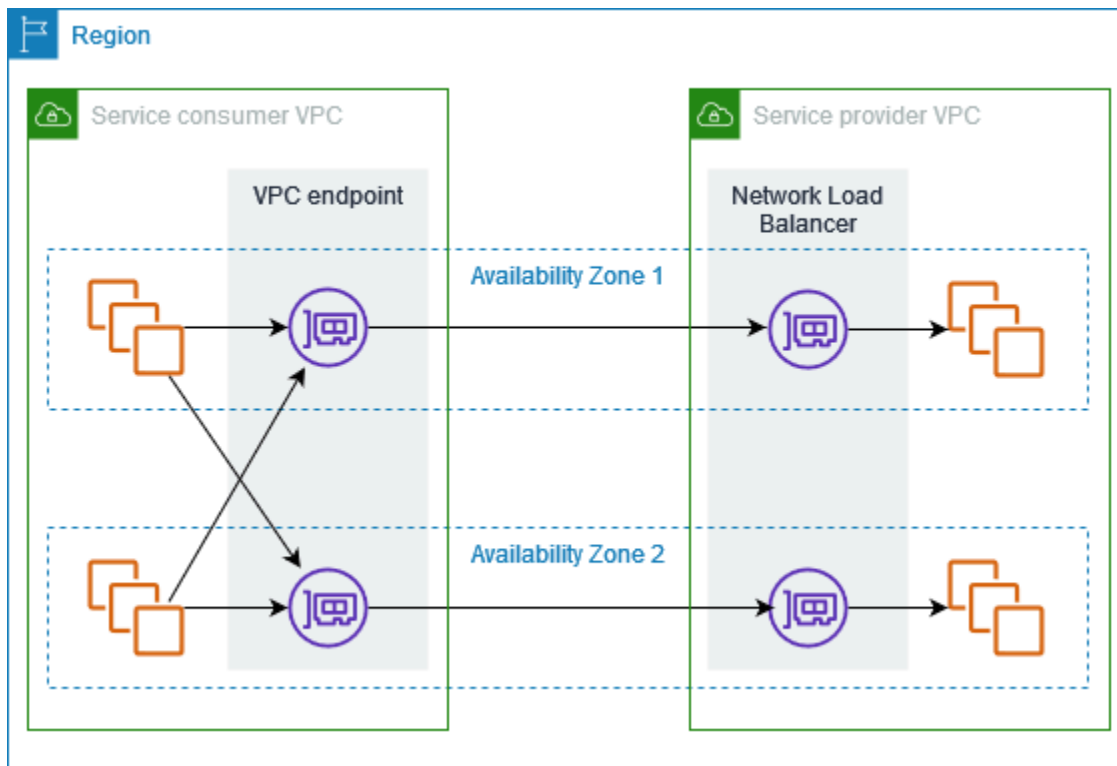
Anda dapat meng-host layanan AWS PrivateLink bertenaga Anda sendiri, yang dikenal sebagai layanan titik akhir, dan membagikannya dengan AWS pelanggan lain.

Daftar Isi

- [Gambaran umum](#)
- [Nama host DNS](#)
- [DNS privat](#)
- [Subnet dan Zona Ketersediaan](#)
- [Cross-Region akses](#)
- [Jenis alamat IP](#)
- [Buat layanan yang didukung oleh AWS PrivateLink](#)
- [Mengkonfigurasi layanan titik akhir](#)
- [Kelola nama DNS untuk layanan titik akhir VPC](#)
- [Menerima peringatan untuk acara layanan titik akhir](#)
- [Menghapus layanan titik akhir](#)

Gambaran umum

Diagram berikut menunjukkan bagaimana Anda berbagi layanan yang dihosting AWS dengan AWS pelanggan lain, dan bagaimana pelanggan tersebut terhubung ke layanan Anda. Sebagai penyedia layanan, Anda membuat Network Load Balancer di VPC Anda sebagai bagian depan layanan. Anda kemudian memilih penyeimbang beban ini saat membuat konfigurasi layanan titik akhir VPC. Anda memberikan izin kepada prinsi AWS pal tertentu sehingga mereka dapat terhubung ke layanan Anda. Sebagai konsumen layanan, pelanggan membuat titik akhir VPC antarmuka, yang membuat koneksi antara subnet yang mereka pilih dari VPC mereka dan layanan titik akhir Anda. Penyeimbang beban menerima permintaan dari konsumen layanan dan mengarahkannya ke target yang menghosting layanan Anda.



Untuk latensi rendah dan ketersediaan tinggi, kami sarankan Anda menyediakan layanan setidaknya di dua Zona Ketersediaan.

Nama host DNS

Ketika penyedia layanan membuat layanan titik akhir VPC, AWS menghasilkan nama host DNS khusus titik akhir untuk layanan tersebut. Nama-nama ini memiliki sintaks berikut:

```
endpoint_service_id.region.vpce.amazonaws.com
```

Berikut ini adalah contoh nama host DNS untuk layanan titik akhir VPC di Wilayah us-east-2:

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

Ketika konsumen layanan membuat titik akhir VPC antarmuka, kami membuat nama DNS Regional dan zonal yang dapat digunakan konsumen layanan untuk berkomunikasi dengan layanan titik akhir. Nama regional memiliki sintaks berikut:

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

Nama zona memiliki sintaks berikut:

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

DNS privat

Penyedia layanan juga dapat mengaitkan nama DNS pribadi untuk layanan titik akhir mereka, sehingga konsumen layanan dapat terus mengakses layanan menggunakan nama DNS yang ada. Jika penyedia layanan mengaitkan nama DNS pribadi dengan layanan titik akhir mereka, maka konsumen layanan dapat mengaktifkan nama DNS pribadi untuk titik akhir antarmuka mereka. Jika penyedia layanan tidak mengaktifkan DNS pribadi, maka konsumen layanan mungkin perlu memperbarui aplikasi mereka untuk menggunakan nama DNS publik dari layanan titik akhir VPC. Untuk informasi selengkapnya, lihat [Kelola nama DNS](#).

Subnet dan Zona Ketersediaan

Layanan titik akhir Anda tersedia di Zona Ketersediaan yang Anda aktifkan untuk Penyeimbang Beban Jaringan. Untuk ketersediaan dan ketahanan yang tinggi, kami sarankan Anda mengaktifkan penyeimbang beban setidaknya di dua Zona Ketersediaan, menerapkan instans EC2 di setiap zona yang diaktifkan, dan mendaftarkan instans ini ke grup target penyeimbang beban Anda.

Anda dapat mengaktifkan penyeimbangan beban lintas zona sebagai alternatif untuk menghosting layanan titik akhir Anda di beberapa Zona Ketersediaan. Namun, konsumen akan kehilangan akses ke layanan titik akhir dari kedua zona jika zona yang menghosting layanan titik akhir gagal. Juga pertimbangkan bahwa ketika Anda mengaktifkan penyeimbangan beban lintas zona untuk Penyeimbang Beban Jaringan, biaya transfer data EC2 berlaku.

Konsumen dapat membuat titik akhir VPC antarmuka di Zona Ketersediaan tempat layanan titik akhir Anda tersedia. Kami membuat antarmuka jaringan titik akhir di setiap subnet yang dikonfigurasi konsumen untuk titik akhir VPC. Kami menetapkan alamat IP ke setiap antarmuka jaringan titik akhir dari subnetnya, berdasarkan jenis alamat IP dari titik akhir VPC. Ketika permintaan menggunakan titik akhir regional untuk layanan titik akhir VPC, kami memilih antarmuka jaringan titik akhir yang sehat, menggunakan algoritma round robin untuk bergantian antara antarmuka jaringan di Zona Ketersediaan yang berbeda. Kami kemudian menyelesaikan lalu lintas ke alamat IP dari antarmuka jaringan titik akhir yang dipilih.

Konsumen dapat menggunakan titik akhir zonal untuk titik akhir VPC jika lebih baik untuk kasus penggunaan mereka untuk menjaga lalu lintas di Zona Ketersediaan yang sama.

Cross-Region akses

Penyedia layanan dapat meng-host layanan di satu Wilayah dan membuatnya tersedia di satu set Wilayah yang didukung. Konsumen layanan memilih Wilayah layanan saat membuat titik akhir.

Izin

- Secara default, entitas IAM tidak memiliki izin untuk membuat layanan titik akhir tersedia di beberapa Wilayah atau mengakses layanan titik akhir di seluruh Wilayah. Untuk memberikan izin yang diperlukan untuk akses lintas wilayah, administrator IAM dapat membuat kebijakan IAM yang mengizinkan tindakan khusus izin. `vpce:AllowMultiRegion`
- Untuk mengontrol Wilayah yang entitas IAM dapat menentukan sebagai Wilayah yang didukung saat membuat layanan titik akhir, gunakan kunci `ec2:VpceSupportedRegion` kondisi.
- Untuk mengontrol Wilayah yang entitas IAM dapat menentukan sebagai Wilayah layanan saat membuat titik akhir VPC, gunakan kunci `ec2:VpceServiceRegion` kondisi.

Pertimbangan-pertimbangan

- Penyedia layanan harus memilih untuk masuk ke Wilayah opt-in sebelum menambahkannya sebagai Wilayah yang didukung untuk layanan titik akhir.
- Layanan titik akhir Anda harus dapat diakses dari Wilayah host. Anda tidak dapat menghapus Region host dari kumpulan Wilayah yang didukung. Untuk redundansi, Anda dapat menerapkan layanan titik akhir Anda di beberapa Wilayah dan mengaktifkan akses lintas wilayah untuk setiap layanan titik akhir.
- Konsumen layanan harus memilih Wilayah opt-in sebelum memilihnya sebagai Wilayah layanan untuk titik akhir. Jika memungkinkan, kami menyarankan agar konsumen layanan mengakses layanan menggunakan konektivitas intra-wilayah alih-alih konektivitas lintas wilayah. Intra-Region konektivitas memberikan latensi yang lebih rendah dan biaya yang lebih rendah.
- Jika penyedia layanan menghapus Wilayah dari kumpulan Wilayah yang didukung, konsumen layanan tidak dapat memilih Wilayah tersebut sebagai Wilayah layanan saat mereka membuat titik akhir baru. Perhatikan bahwa ini tidak mempengaruhi akses ke layanan titik akhir dari titik akhir yang ada yang menggunakan Wilayah ini sebagai Wilayah layanan.
- Untuk ketersediaan tinggi, penyedia harus menggunakan setidaknya dua Zona Ketersediaan. Cross-Region akses tidak mengharuskan penyedia dan konsumen menggunakan Zona Ketersediaan yang sama.

- Cross-Region akses tidak didukung untuk Zona Ketersediaan berikut: use1-az3, usw1-az2, apne1-az3, apne2-az2, dan apne2-az4.
- Dengan akses lintas wilayah, AWS PrivateLink mengelola failover antara Availability Zone. Itu tidak mengelola failover di seluruh Wilayah.
- Cross-Region akses tidak didukung untuk Network Load Balancers dengan nilai kustom yang dikonfigurasi untuk batas waktu idle TCP.
- Cross-Region akses tidak didukung dengan fragmentasi UDP.
- Cross-Region akses hanya didukung untuk layanan yang Anda bagikan melalui AWS PrivateLink.

Jenis alamat IP

Penyedia layanan dapat membuat titik akhir layanan mereka tersedia untuk konsumen layanan melalui IPv4, IPv6, atau IPv4 dan IPv6, bahkan jika server backend mereka hanya mendukung IPv4. Jika Anda mengaktifkan dukungan dualstack, konsumen yang sudah ada dapat terus menggunakan IPv4 untuk mengakses layanan Anda dan konsumen baru dapat memilih untuk menggunakan IPv6 untuk mengakses layanan Anda.

Jika antarmuka titik akhir VPC mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika antarmuka titik akhir VPC mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan titik akhir tidak dapat dijangkau dari internet. Jika Anda menjelaskan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu denyAllIgwTraffic diaktifkan.

Persyaratan untuk mengaktifkan IPv6 untuk layanan titik akhir

- VPC dan subnet untuk layanan endpoint harus memiliki blok IPv6 CIDR terkait.
- Semua Penyeimbang Beban Jaringan untuk layanan titik akhir harus menggunakan jenis alamat IP dualstack. Target tidak perlu mendukung lalu lintas IPv6. Jika layanan memproses alamat IP sumber dari header protokol proxy versi 2, itu harus memproses alamat IPv6.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir antarmuka

- Layanan endpoint harus mendukung permintaan IPv6.
- Jenis alamat IP dari titik akhir antarmuka harus kompatibel dengan subnet untuk titik akhir antarmuka, seperti yang dijelaskan di sini:

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

Jenis alamat IP catatan DNS untuk titik akhir antarmuka

Jenis alamat IP catatan DNS yang didukung oleh titik akhir antarmuka menentukan catatan DNS yang kita buat. Jenis alamat IP catatan DNS dari titik akhir antarmuka harus kompatibel dengan jenis alamat IP dari titik akhir antarmuka, seperti yang dijelaskan di sini:

- IPv4 — Buat catatan A untuk nama DNS pribadi, Regional, dan zonal. Jenis alamat IP harus IPv4 atau Dualstack.
- IPv6 — Buat catatan AAAA untuk nama DNS pribadi, Regional, dan zonal. Jenis alamat IP harus IPv6 atau Dualstack.
- Dualstack — Buat catatan A dan AAAA untuk nama DNS pribadi, Regional, dan zonal. Jenis alamat IP harus Dualstack.

Buat layanan yang didukung oleh AWS PrivateLink

Anda dapat membuat layanan Anda sendiri yang didukung oleh AWS PrivateLink, yang dikenal sebagai layanan titik akhir. Anda adalah penyedia layanan, dan prinsipal yang membuat koneksi ke layanan Anda adalah konsumen layanan.

Layanan Endpoint memerlukan Network Load Balancer atau Gateway Load Balancer. Penyeimbang beban menerima permintaan dari konsumen layanan dan mengarahkannya ke layanan Anda. Dalam hal ini, Anda akan membuat layanan endpoint menggunakan Network Load Balancer. Untuk informasi selengkapnya tentang membuat layanan titik akhir menggunakan Gateway Load Balancer, lihat [Akses peralatan virtual](#).

Daftar Isi

- [Pertimbangan-pertimbangan](#)
- [Prasyarat](#)
- [Membuat layanan titik akhir](#)

- [Jadikan layanan endpoint Anda tersedia untuk konsumen layanan](#)
- [Menghubungkan ke layanan titik akhir sebagai konsumen layanan](#)

Pertimbangan-pertimbangan

- Layanan titik akhir tersedia di Wilayah tempat Anda membuatnya. Konsumen dapat mengakses layanan Anda dari Wilayah lain jika Anda mengaktifkan [akses Lintas wilayah](#), atau jika mereka menggunakan peering VPC atau gateway transit.
- Ketika konsumen layanan mengambil informasi tentang layanan titik akhir, mereka hanya dapat melihat Zona Ketersediaan yang mereka miliki bersama dengan penyedia layanan. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Zona Ketersediaan, seperti us-east-1a, mungkin dipetakan ke Zona Ketersediaan fisik yang berbeda di masing-masing Akun AWS. Anda dapat menggunakan ID AZ untuk secara konsisten mengidentifikasi Zona Ketersediaan untuk layanan Anda. Untuk informasi selengkapnya, lihat ID [AZ](#) di Panduan Pengguna Amazon EC2.
- Ketika konsumen layanan mengirim lalu lintas ke layanan melalui titik akhir antarmuka, alamat IP sumber yang diberikan ke aplikasi adalah alamat IP pribadi dari node penyeimbang beban, bukan alamat IP konsumen layanan. Jika Anda mengaktifkan protokol proxy pada penyeimbang beban, Anda dapat memperoleh alamat konsumen layanan dan ID titik akhir antarmuka dari header protokol proxy. Untuk informasi selengkapnya, lihat Protokol [Proxy](#) di Panduan Pengguna untuk Penyeimbang Beban Jaringan.
- Network Load Balancer dapat dikaitkan dengan layanan titik akhir tunggal, tetapi layanan endpoint dapat dikaitkan dengan beberapa Network Load Balancer.
- Jika layanan titik akhir dikaitkan dengan beberapa Network Load Balancer, setiap antarmuka jaringan titik akhir dikaitkan dengan satu penyeimbang beban. Ketika koneksi pertama dari antarmuka jaringan titik akhir dimulai, kami memilih salah satu Penyeimbang Beban Jaringan di Zona Ketersediaan yang sama dengan antarmuka jaringan titik akhir secara acak. Semua permintaan koneksi berikutnya dari antarmuka jaringan titik akhir ini menggunakan penyeimbang beban yang dipilih. Sebaiknya gunakan konfigurasi pendengar dan grup target yang sama untuk semua penyeimbang beban untuk layanan titik akhir, sehingga konsumen dapat menggunakan layanan titik akhir dengan sukses terlepas dari penyeimbang beban mana yang dipilih.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat [AWS PrivateLink kuota](#).

Prasyarat

- Buat VPC untuk layanan titik akhir Anda dengan setidaknya satu subnet di setiap Zona Ketersediaan tempat layanan harus tersedia.
- Untuk memungkinkan konsumen layanan membuat titik akhir VPC antarmuka IPv6 untuk layanan titik akhir Anda, VPC dan subnet harus memiliki blok IPv6 CIDR terkait.
- Buat Network Load Balancer di VPC Anda. Pilih satu subnet per Zona Ketersediaan di mana layanan harus tersedia untuk konsumen layanan. Untuk latensi rendah dan toleransi kesalahan, kami sarankan Anda menyediakan layanan setidaknya di dua Zona Ketersediaan di Wilayah.
- Jika Network Load Balancer Anda memiliki grup keamanan, itu harus mengizinkan lalu lintas masuk dari alamat IP klien. Atau, Anda dapat menonaktifkan evaluasi aturan grup keamanan masuk untuk lalu lintas melalui AWS PrivateLink. Untuk informasi selengkapnya, lihat [Grup keamanan](#) di Panduan Pengguna untuk Penyeimbang Beban Jaringan.
- Untuk mengaktifkan layanan titik akhir Anda menerima permintaan IPv6, Network Load Balancers harus menggunakan jenis alamat IP dualstack. Target tidak perlu mendukung lalu lintas IPv6. Untuk informasi selengkapnya, lihat [Jenis alamat IP](#) di Panduan Pengguna untuk Penyeimbang Beban Jaringan.

Jika Anda memproses alamat IP sumber dari header protokol proxy versi 2, verifikasi bahwa Anda dapat memproses alamat IPv6.

- Luncurkan instans di setiap Zona Ketersediaan di mana layanan harus tersedia dan daftarkan dengan grup target penyeimbang beban. Jika Anda tidak meluncurkan instans di semua Zona Ketersediaan yang diaktifkan, Anda dapat mengaktifkan penyeimbangan beban lintas zona untuk mendukung konsumen layanan yang menggunakan nama host DNS zona untuk mengakses layanan. Biaya transfer data regional berlaku saat Anda mengaktifkan penyeimbangan beban lintas zona. Untuk informasi selengkapnya, lihat [Cross-zone penyeimbangan beban](#) di Panduan Pengguna untuk Penyeimbang Beban Jaringan.

Membuat layanan titik akhir

Gunakan prosedur berikut untuk membuat layanan titik akhir menggunakan Network Load Balancer.

Untuk membuat layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.

3. Pilih **Buat layanan titik akhir**.
4. Untuk jenis penyeimbang beban, pilih **Jaringan**.
5. Untuk penyeimbang beban yang tersedia, pilih **Network Load Balancers** untuk dikaitkan dengan layanan titik akhir. Untuk melihat Zona Ketersediaan yang diaktifkan untuk penyeimbang beban yang Anda pilih, lihat **Detail penyeimbang beban** yang dipilih, **Zona Ketersediaan Ter masuk**. Layanan titik akhir Anda akan tersedia di Zona Ketersediaan ini.
6. (Opsional) Untuk membuat layanan titik akhir Anda tersedia dari Wilayah selain Wilayah tempat layanan dihosting, pilih Wilayah dari Wilayah Layanan. Untuk informasi selengkapnya, lihat [the section called “Cross-Region akses”](#).
7. Untuk Memerlukan penerimaan untuk titik akhir, pilih **Penerimaan diperlukan** untuk mengharuskan permintaan koneksi ke layanan titik akhir Anda diterima secara manual. Jika tidak, permintaan ini diterima secara otomatis.
8. Untuk Aktifkan nama DNS pribadi, pilih **Kaitkan nama DNS pribadi** dengan layanan untuk mengaitkan nama DNS pribadi yang dapat digunakan konsumen layanan untuk mengakses layanan Anda, lalu masukkan nama DNS pribadi. Jika tidak, konsumen layanan dapat menggunakan nama DNS khusus titik akhir yang disediakan oleh AWS. Sebelum konsumen layanan dapat menggunakan nama DNS pribadi, penyedia layanan harus memverifikasi bahwa mereka memiliki domain. Untuk informasi selengkapnya, lihat [Kelola nama DNS](#).
9. Untuk jenis alamat IP yang didukung, lakukan salah satu hal berikut:
 - Pilih **IPv4** — Aktifkan layanan titik akhir untuk menerima permintaan IPv4.
 - Pilih **IPv6** — Aktifkan layanan titik akhir untuk menerima permintaan IPv6.
 - Pilih **IPv4 dan IPv6** — Aktifkan layanan titik akhir untuk menerima permintaan IPv4 dan IPv6.
10. (Opsional) Untuk menambahkan tanda, pilih **Tambahkan tanda baru** dan masukkan kunci dan nilai tanda.
11. Pilih **Buat**.

Untuk membuat layanan titik akhir menggunakan baris perintah

- [buat-konfigurasi layanan-endpoint-vpc-\(\)](#) AWS CLI
- [New-EC2VpcEndpointServiceConfiguration](#) (Alat untuk Windows PowerShell)

Jadikan layanan endpoint Anda tersedia untuk konsumen layanan

AWS prinsipal dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat antarmuka titik akhir VPC. Penyedia layanan harus melakukan hal berikut untuk membuat layanan mereka tersedia bagi konsumen layanan.

- Tambahkan izin yang memungkinkan setiap konsumen layanan terhubung ke layanan titik akhir Anda. Untuk informasi selengkapnya, lihat [the section called “Kelola izin”](#).
- Berikan nama layanan Anda dan Zona Ketersediaan yang didukung kepada konsumen layanan sehingga mereka dapat membuat titik akhir antarmuka untuk terhubung ke layanan Anda. Untuk informasi selengkapnya, lihat [the section called “Menghubungkan ke layanan titik akhir sebagai konsumen layanan”](#).
- Terima permintaan koneksi titik akhir dari konsumen layanan. Untuk informasi selengkapnya, lihat [the section called “Menerima atau tolak permintaan koneksi”](#).

Menghubungkan ke layanan titik akhir sebagai konsumen layanan

Konsumen layanan menggunakan prosedur berikut untuk membuat titik akhir antarmuka untuk terhubung ke layanan titik akhir Anda.

Untuk membuat titik akhir antarmuka menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih layanan Endpoint yang menggunakan NLB dan GW LB.
5. Untuk Nama layanan, masukkan nama layanan (misalnya, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), lalu pilih Verifikasi layanan.
6. (Opsional) Untuk menyambung ke layanan titik akhir yang tersedia di Wilayah selain Wilayah titik akhir, pilih Wilayah Layanan, Aktifkan titik akhir Lintas Wilayah, lalu pilih Wilayah. Untuk informasi selengkapnya, lihat [the section called “Cross-Region akses”](#).
7. Untuk VPC, pilih VPC tempat Anda akan mengakses layanan titik akhir.
8. Untuk Subnet, pilih subnet tempat untuk membuat antarmuka jaringan titik akhir.
9. Untuk jenis alamat IP, pilih dari opsi berikut:

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

10. Untuk tipe IP catatan DNS, pilih dari opsi berikut:

- IPv4 — Buat catatan A untuk nama DNS pribadi, Regional, dan zonal. Jenis alamat IP harus IPv4 atau Dualstack.
- IPv6 — Buat catatan AAAA untuk nama DNS pribadi, Regional, dan zonal. Jenis alamat IP harus IPv6 atau Dualstack.
- Dualstack — Buat catatan A dan AAAA untuk nama DNS pribadi, Regional, dan zonal. Jenis alamat IP harus Dualstack.
- Layanan ditentukan — Buat catatan A untuk nama DNS pribadi, Regional, dan zona dan catatan AAAA untuk nama DNS Regional dan zonal. Jenis alamat IP harus Dualstack.

11. Untuk grup keamanan, pilih grup keamanan yang akan diasosiasikan dengan antarmuka jaringan titik akhir.

12. Pilih Buat titik akhir.

Untuk membuat titik akhir antarmuka menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Mengkonfigurasi layanan titik akhir

Setelah Anda membuat layanan titik akhir, Anda dapat memperbarui konfigurasinya.

Tugas

- [Kelola izin](#)

- [Menerima atau tolak permintaan koneksi](#)
- [Kelola penyeimbang beban](#)
- [Mengaitkan nama DNS pribadi](#)
- [Ubah Wilayah yang didukung](#)
- [Ubah jenis alamat IP yang didukung](#)
- [Kelola tanda](#)

Kelola izin

Kombinasi pengaturan izin dan penerimaan membantu Anda mengontrol konsumen layanan (AWS prinsipal) mana yang dapat mengakses layanan titik akhir Anda. Misalnya, Anda dapat memberikan izin kepada prinsipal tertentu yang Anda percayai dan secara otomatis menerima semua permintaan koneksi, atau Anda dapat memberikan izin ke grup prinsipal yang lebih luas dan secara manual menerima permintaan koneksi tertentu yang Anda percayai.

Secara default, layanan titik akhir Anda tidak tersedia untuk konsumen layanan. Anda harus menambahkan izin yang memungkinkan prinsipal AWS tertentu untuk membuat titik akhir VPC antarmuka untuk terhubung ke layanan titik akhir Anda. Untuk menambahkan izin untuk prinsi AWS pal, Anda memerlukan Nama Sumber Daya Amazon (ARN). Daftar berikut mencakup contoh ARN untuk prinsipal yang didukung AWS .

ARN untuk AWS utama

Akun AWS (termasuk semua prinsipal dalam akun)

`arn:aws:iam: ::root account_id`

Peran

`arn:aws:iam: ::role/ account_id role_name`

Pengguna

`arn:aws:iam: ::penggun/ account_id user_name`

Semua kepala sekolah di semua Akun AWS

*

Pertimbangan-pertimbangan

- Jika Anda memberikan izin kepada semua orang untuk mengakses layanan titik akhir dan mengonfigurasi layanan titik akhir untuk menerima semua permintaan, penyeimbang beban Anda akan menjadi publik meskipun tidak memiliki alamat IP publik.
- Jika Anda menghapus izin, itu tidak mempengaruhi koneksi yang ada antara titik akhir dan layanan yang sebelumnya diterima.

Untuk mengelola izin untuk layanan titik akhir Anda menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir dan pilih tab Izinkan prinsipal.
4. Untuk menambahkan izin, pilih Izinkan prinsipal. Untuk menambah Kepala Sekolah, masukkan ARN kepala sekolah. Untuk menambahkan prinsipal lain, pilih Tambah pokok. Setelah selesai menambahkan prinsipal, pilih Izinkan prinsipal.
5. Untuk menghapus izin, pilih prinsipal dan pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

Untuk menambahkan izin untuk layanan titik akhir Anda menggunakan baris perintah

- [modify-vpc-izin-layanan-endpoint-\(\)](#)AWS CLI
- [Edit-EC2EndpointServicePermission](#)(Alat untuk Windows PowerShell)

Menerima atau tolak permintaan koneksi

Kombinasi pengaturan izin dan penerimaan membantu Anda mengontrol konsumen layanan (AWS prinsipal) mana yang dapat mengakses layanan titik akhir Anda. Misalnya, Anda dapat memberikan izin kepada prinsipal tertentu yang Anda percayai dan secara otomatis menerima semua permintaan koneksi, atau Anda dapat memberikan izin ke grup prinsipal yang lebih luas dan secara manual menerima permintaan koneksi tertentu yang Anda percayai.

Anda dapat mengonfigurasi layanan titik akhir untuk menerima permintaan koneksi secara otomatis. Jika tidak, Anda harus menerima atau menolaknya secara manual. Jika Anda tidak menerima permintaan koneksi, konsumen layanan tidak dapat mengakses layanan titik akhir Anda.

Jika Anda memberikan izin kepada semua orang untuk mengakses layanan titik akhir dan mengonfigurasi layanan titik akhir untuk menerima semua permintaan, penyeimbang beban Anda akan menjadi publik meskipun tidak memiliki alamat IP publik.

Anda dapat menerima pemberitahuan ketika permintaan koneksi diterima atau ditolak. Untuk informasi selengkapnya, lihat [the section called “Menerima peringatan untuk acara layanan titik akhir”](#).

Untuk mengubah pengaturan penerimaan menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Pilih Tindakan, Ubah pengaturan penerimaan titik akhir.
5. Pilih atau hapus Penerimaan diperlukan.
6. Pilih Save changes (Simpan perubahan)

Untuk mengubah pengaturan penerimaan menggunakan baris perintah

- [modify-](#) vpc-konfigurasi-layanan-endpoint-()AWS CLI
- [Edit-EC2VpcEndpointServiceConfiguration](#)(Alat untuk Windows PowerShell)

Untuk menerima atau menolak permintaan koneksi menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Dari tab Koneksi titik akhir, pilih koneksi titik akhir.
5. Untuk menerima permintaan koneksi, pilih Tindakan, Terima permintaan koneksi titik akhir. Saat diminta konfirmasi, masukkan **accept** lalu pilih Terima.
6. Untuk menolak permintaan koneksi, pilih Tindakan, Tolak permintaan koneksi titik akhir. Saat diminta konfirmasi, masukkan **reject** lalu pilih Tolak.

Untuk menerima atau menolak permintaan koneksi menggunakan baris perintah

- [sambungan titik akhir accept-vpc-atau sambungan titik akhir tolak-vpc-\(\)](https://docs.aws.amazon.com/cli/latest/reference/ec2/reject-vpc-endpoint-connections.html) <https://docs.aws.amazon.com/cli/latest/reference/ec2/reject-vpc-endpoint-connections.html> AWS CLI
- [Approve-EC2EndpointConnection](#) atau [Deny-EC2EndpointConnection](#) (Alat untuk Windows PowerShell)

Kelola penyeimbang beban

Anda dapat mengelola penyeimbang beban yang terkait dengan layanan titik akhir Anda. Anda tidak dapat memutuskan penyeimbang beban jika ada titik akhir yang terhubung ke layanan titik akhir Anda.

Jika Anda mengaktifkan Availability Zone lain untuk penyeimbang beban, Availability Zone akan muncul di bawah tab Load Balancers pada halaman layanan Endpoint. Namun, itu tidak akan diaktifkan untuk layanan titik akhir atau terdaftar di tab Detail layanan titik akhir Anda di Konsol Manajemen AWS. Anda perlu mengaktifkan layanan titik akhir untuk Zona Ketersediaan baru.

Mungkin perlu beberapa menit agar Zona Ketersediaan load balancer siap untuk layanan endpoint Anda. Jika Anda menggunakan otomatisasi, sebaiknya tambahkan waktu tunggu dalam proses otomatisasi sebelum mengaktifkan layanan titik akhir untuk Zona Ketersediaan baru.

Untuk mengelola penyeimbang beban untuk layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Pilih Tindakan, Mengasosiasikan atau lepaskan penyeimbang beban.
5. Ubah konfigurasi layanan titik akhir sesuai kebutuhan. Contoh:
 - Pilih kotak centang untuk penyeimbang beban untuk mengaitkannya dengan layanan titik akhir.
 - Kosongkan kotak centang penyeimbang beban untuk memisahkannya dari layanan titik akhir. Anda harus memilih setidaknya satu penyeimbang beban.
6. Pilih Save changes (Simpan perubahan)

Layanan titik akhir akan diaktifkan untuk setiap Zona Ketersediaan baru yang Anda tambahkan ke penyeimbang beban Anda. Zona Ketersediaan baru tercantum di bawah tab **Load Balancers** dan tab **Detail** dari layanan titik akhir.

Setelah Anda mengaktifkan Zona Ketersediaan untuk layanan titik akhir, konsumen layanan dapat menambahkan subnet dari Zona Ketersediaan tersebut ke titik akhir VPC antarmuka mereka.

Untuk mengelola penyeimbang beban untuk layanan titik akhir Anda menggunakan baris perintah

- [modify-vpc-konfigurasi-layanan-endpoint-\(\)](#) AWS CLI
- [Edit-EC2VpcEndpointServiceConfiguration](#) (Alat untuk Windows PowerShell)

Untuk mengaktifkan layanan titik akhir di Zona Ketersediaan yang baru-baru ini diaktifkan untuk penyeimbang beban, cukup panggil perintah dengan ID layanan titik akhir.

Mengaitkan nama DNS pribadi

Anda dapat mengaitkan nama DNS pribadi dengan layanan titik akhir Anda. Setelah Anda mengaitkan nama DNS pribadi, Anda harus memperbarui entri untuk domain di server DNS Anda. Sebelum konsumen layanan dapat menggunakan nama DNS pribadi, penyedia layanan harus memverifikasi bahwa mereka memiliki domain. Untuk informasi selengkapnya, lihat [Kelola nama DNS](#).

Untuk mengubah nama DNS pribadi layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan **Endpoint**.
3. Pilih layanan titik akhir.
4. Pilih **Tindakan**, **Ubah nama DNS pribadi**.
5. Pilih **Kaitkan nama DNS pribadi dengan layanan** dan masukkan nama DNS pribadi.
 - Nama domain harus menggunakan huruf kecil.
 - Anda dapat menggunakan wildcard dalam nama domain (misalnya, ***.myexampleservice.com**).
6. Pilih **Simpan perubahan**.

7. Nama DNS pribadi siap digunakan oleh konsumen layanan ketika status verifikasi di verifikasi. Jika status verifikasi berubah, permintaan koneksi baru ditolak tetapi koneksi yang ada tidak terpengaruh.

Untuk mengubah nama DNS pribadi layanan titik akhir menggunakan baris perintah

- [modify-](#) vpc-konfigurasi-layanan-endpoint-()AWS CLI
- [Edit-EC2VpcEndpointServiceConfiguration](#)(Alat untuk Windows PowerShell)

Untuk memulai proses verifikasi domain menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Pilih Tindakan, Verifikasi kepemilikan domain untuk nama DNS pribadi.
5. Saat diminta konfirmasi, masukkan **verify** lalu pilih Verifikasi.

Untuk memulai proses verifikasi domain menggunakan baris perintah

- [start-vpc-](#) endpoint-layanan-privat-dns-verifikasi ()AWS CLI
- [Start-EC2VpcEndpointServicePrivateDnsVerification](#)(Alat untuk Windows PowerShell)

Ubah Wilayah yang didukung

Anda dapat memodifikasi kumpulan Wilayah yang didukung untuk layanan titik akhir Anda. Sebelum Anda dapat menambahkan Wilayah opt-in, Anda harus ikut serta. Anda tidak dapat menghapus Wilayah yang menghosting layanan titik akhir Anda.

Setelah Anda menghapus Wilayah, konsumen layanan tidak dapat membuat titik akhir baru yang menentukannya sebagai Wilayah layanan. Menghapus Wilayah tidak mempengaruhi titik akhir yang ada yang menentukannya sebagai Wilayah layanan. Saat Anda menghapus Wilayah, kami sarankan Anda menolak koneksi titik akhir yang ada dari Wilayah tersebut.

Untuk mengubah Wilayah yang didukung untuk layanan titik akhir Anda

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.

2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Pilih Tindakan, Ubah Wilayah yang didukung.
5. Pilih dan hapus pilihan Wilayah sesuai kebutuhan.
6. Pilih Simpan perubahan.

Ubah jenis alamat IP yang didukung

Anda dapat mengubah jenis alamat IP yang didukung oleh layanan titik akhir Anda.

Pertimbangan

Untuk mengaktifkan layanan titik akhir Anda menerima permintaan IPv6, Network Load Balancers harus menggunakan jenis alamat IP dualstack. Target tidak perlu mendukung lalu lintas IPv6. Untuk informasi selengkapnya, lihat [Jenis alamat IP](#) di Panduan Pengguna untuk Penyeimbang Beban Jaringan.

Untuk memodifikasi jenis alamat IP yang didukung menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir VPC.
4. Pilih Tindakan, Ubah jenis alamat IP yang didukung.
5. Untuk jenis alamat IP yang didukung, lakukan salah satu hal berikut:
 - Pilih IPv4 — Aktifkan layanan titik akhir untuk menerima permintaan IPv4.
 - Pilih IPv6 — Aktifkan layanan titik akhir untuk menerima permintaan IPv6.
 - Pilih IPv4 dan IPv6 — Aktifkan layanan titik akhir untuk menerima permintaan IPv4 dan IPv6.
6. Pilih Simpan perubahan.

Untuk memodifikasi jenis alamat IP yang didukung menggunakan baris perintah

- [modify-](#) vpc-konfigurasi-layanan-endpoint-()AWS CLI
- [Edit-EC2VpcEndpointServiceConfiguration](#)(Alat untuk Windows PowerShell)

Kelola tanda

Anda dapat menandai sumber daya Anda untuk membantu mengidentifikasi mereka atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk mengelola tag untuk layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir VPC.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag yang akan ditambahkan, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag untuk koneksi titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir VPC dan kemudian pilih tab Koneksi titik akhir.
4. Pilih koneksi titik akhir dan kemudian pilih Tindakan, Kelola tag.
5. Untuk setiap tag yang akan ditambahkan, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag untuk izin layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir VPC dan kemudian pilih tab Izinkan prinsipal.
4. Pilih prinsipal dan kemudian pilih Tindakan, Kelola tag.

5. Untuk setiap tag yang akan ditambahkan, pilih **Tambahkan tag baru** dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih **Hapus** di sebelah kanan kunci tag dan nilai.
7. Pilih **Simpan**.

Untuk menambah dan menghapus tag menggunakan baris perintah

- [buat-tag](#) dan hapus tag (`()`) AWS CLI
- [New-EC2Tag](#) dan [Remove-EC2Tag](#) (Alat untuk Windows PowerShell)

Kelola nama DNS untuk layanan titik akhir VPC

Penyedia layanan dapat mengonfigurasi nama DNS pribadi untuk layanan endpoint mereka.

Misalkan penyedia layanan membuat layanan mereka tersedia melalui titik akhir publik dan sebagai layanan titik akhir. Jika penyedia layanan menggunakan nama DNS dari titik akhir publik sebagai nama DNS pribadi dari layanan titik akhir, maka konsumen layanan dapat mengakses titik akhir publik atau layanan titik akhir menggunakan aplikasi klien yang sama, tanpa modifikasi. Jika permintaan berasal dari VPC konsumen layanan, server DNS pribadi menyelesaikan nama DNS ke alamat IP antarmuka jaringan titik akhir. Jika tidak, server DNS publik menyelesaikan nama DNS ke titik akhir publik.

Sebelum Anda dapat mengonfigurasi nama DNS pribadi untuk layanan titik akhir Anda, Anda harus membuktikan bahwa Anda memiliki domain dengan melakukan pemeriksaan verifikasi kepemilikan domain.

Pertimbangan-pertimbangan

- Layanan endpoint hanya dapat memiliki satu nama DNS pribadi.
- Ketika konsumen membuat titik akhir antarmuka untuk terhubung ke layanan Anda, kami membuat zona yang dihosting pribadi dan mengaitkannya dengan VPC konsumen layanan. Kami membuat catatan CNAME di zona host pribadi yang memetakan nama DNS pribadi dari layanan titik akhir ke nama DNS regional dari titik akhir VPC. Ketika konsumen mengirim permintaan ke nama DNS publik layanan, server DNS pribadi menyelesaikan permintaan ke alamat IP antarmuka jaringan titik akhir.
- Untuk memverifikasi domain, Anda harus memiliki nama host publik atau penyedia DNS publik.

- Anda dapat memverifikasi domain subdomain. Misalnya, Anda dapat memverifikasi `example.com`, bukan `example.com`. Setiap label DNS dapat memiliki hingga 63 karakter dan seluruh nama domain tidak boleh melebihi panjang total 255 karakter.

Jika Anda menambahkan subdomain tambahan, Anda harus memverifikasi subdomain, atau domain tersebut. Misalnya, katakanlah Anda memiliki `example.com`, dan `example.com` terverifikasi. Anda sekarang menambahkan `b.example.com` sebagai nama DNS pribadi. Anda harus memverifikasi `example.com` atau `b.example.com` sebelum konsumen layanan dapat menggunakan nama tersebut.

- Nama DNS pribadi tidak didukung untuk titik akhir Gateway Load Balancer.

Verifikasi kepemilikan domain

Domain Anda dikaitkan dengan kumpulan catatan layanan nama domain (DNS) yang Anda kelola melalui penyedia DNS Anda. Catatan TXT adalah tipe catatan DNS yang menyediakan informasi tambahan tentang domain Anda. Ini terdiri dari nama dan nilai. Sebagai bagian dari proses verifikasi, Anda harus menambahkan catatan TXT ke server DNS untuk domain publik Anda.

Verifikasi kepemilikan domain selesai ketika kami mendeteksi keberadaan catatan TXT di pengaturan DNS domain Anda.

Setelah menambahkan catatan, Anda dapat memeriksa status proses verifikasi domain menggunakan konsol Amazon VPC. Di panel navigasi, pilih layanan **Endpoint**. Pilih layanan titik akhir dan periksa nilai status verifikasi **Domain** di tab **Detail**. Jika verifikasi domain tertunda, tunggu beberapa menit dan segarkan layar. Jika diperlukan, Anda dapat memulai proses verifikasi secara manual. Pilih **Tindakan**, **Verifikasi kepemilikan domain** untuk nama DNS pribadi.

Nama DNS pribadi siap digunakan oleh konsumen layanan ketika status verifikasi di **verifikasi**. Jika status verifikasi berubah, permintaan koneksi baru ditolak tetapi koneksi yang ada tidak terpengaruh.

Jika status verifikasi gagal, lihat [the section called “Memecahkan masalah verifikasi domain”](#).

Dapatkan nama dan nilainya

Kami memberi Anda nama dan nilai yang Anda gunakan dalam catatan TXT. Misalnya, informasi tersedia di Konsol Manajemen AWS. Pilih layanan titik akhir dan lihat **Nama verifikasi domain** dan nilai verifikasi domain pada tab **Detail** untuk layanan titik akhir. Anda juga dapat menggunakan [AWS CLI perintah](#) `describe-vpc-endpoint-service-configuration` berikut untuk mengambil informasi tentang konfigurasi nama DNS pribadi untuk layanan titik akhir yang ditentukan.

```
aws ec2 describe-vpc-endpoint-service-configurations \
  --service-ids vpce-svc-071afff70666e61e0 \
  --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

Berikut ini adalah output contoh. Anda akan menggunakan Value dan Name ketika Anda membuat catatan TXT.

```
[
  {
    "State": "pendingVerification",
    "Type": "TXT",
    "Value": "vpce:l6p0ERxlTt45jevFwOCp",
    "Name": "_6e86v84tggqubxbwii1m"
  }
]
```

Misalnya, misalkan nama domain Anda adalah `example.com` dan itu Value dan seperti Name yang ditunjukkan pada contoh output sebelumnya. Tabel berikut adalah contoh pengaturan catatan TXT.

Nama	Tipe	Nilai
_6e86v84tggqubxbwii1m.example.com	TXT	vpce:l6p0 ERxlTt45jevFwOCp

Sebaiknya gunakan Name sebagai subdomain rekaman karena nama domain dasar mungkin sudah digunakan. Namun, jika penyedia DNS Anda tidak mengizinkan nama catatan DNS berisi garis bawah, Anda dapat menghilangkan “_6e86v84tggqubxbwii1m” dan cukup gunakan “example.com” di catatan TXT.

Setelah kami memverifikasi “_6e86v84tggqubxbwii1m.example.com”, konsumen layanan dapat menggunakan “example.com” atau subdomain (misalnya, “service.example.com” atau “my.service.example.com”).

Menambahkan catatan TXT ke server DNS domain Anda

Prosedur untuk menambahkan catatan TXT ke server DNS domain tergantung pada siapa yang menyediakan layanan DNS Anda. Penyedia DNS Anda mungkin Amazon Route 53 atau pendaftar nama domain lainnya.

Amazon Route 53

Buat catatan untuk zona publik yang dihosting menggunakan kebijakan perutean sederhana. Gunakan nilai berikut:

- Untuk Nama rekaman masukkan domain atau subdomain.
- Untuk Tipe catatan, pilih TXT.
- Untuk Value/Route lalu lintas ke, masukkan nilai verifikasi domain.
- Untuk TTL (detik), masukkan **1800**.

Untuk informasi selengkapnya, lihat [Membuat catatan menggunakan konsol](#) di Panduan Pengembang Amazon Route 53.

Prosedur umum

Buka situs web untuk penyedia DNS Anda dan masuk ke akun Anda. Temukan halaman untuk memperbarui catatan DNS untuk domain Anda. Tambahkan catatan TXT dengan nama dan nilai yang kami berikan. Diperlukan waktu hingga 48 jam agar pembaruan catatan DNS berlaku, tetapi seringkali berlaku lebih cepat.

Untuk petunjuk yang lebih spesifik, lihat dokumentasi dari penyedia DNS Anda. Tabel berikut menyediakan tautan ke dokumentasi untuk beberapa penyedia DNS umum. Daftar ini tidak dimaksudkan untuk menjadi komprehensif, juga tidak dimaksudkan sebagai rekomendasi produk atau layanan yang disediakan oleh perusahaan-perusahaan ini.

DNS/Hosting penyedia	Tautan dokumentasi
GoDaddy	Menambahkan catatan TXT
Dreamhost	Menambahkan catatan DNS khusus
Cloudflare	Kelola catatan DNS
HostGator	Kelola Catatan DNS dengan HostGator/eNom
Namecheap	Bagaimana cara menambahkan TXT/SPF/DKIM/DMARC catatan untuk domain saya?
Names.co.uk	Mengubah setelan DNS domain

DNS/Hosting penyedia	Tautan dokumentasi
Wix	Menambahkan atau Memperbarui Catatan TXT di Akun Wix Anda

Periksa apakah catatan TXT diterbitkan

Anda dapat memverifikasi bahwa catatan TXT verifikasi kepemilikan domain nama DNS pribadi Anda dipublikasikan dengan benar ke server DNS Anda menggunakan langkah-langkah berikut. Anda akan menjalankan nslookup perintah, yang tersedia untuk Windows dan Linux.

Anda akan menanyakan server DNS yang melayani domain Anda karena server tersebut berisi informasi terbaru untuk domain Anda. Informasi domain Anda membutuhkan waktu untuk disebarluaskan ke server DNS lainnya.

Untuk memverifikasi bahwa catatan TXT Anda dipublikasikan ke server DNS Anda

1. Temukan server nama untuk domain Anda menggunakan perintah berikut.

```
nslookup -type=NS example.com
```

Output mencantumkan server nama yang melayani domain Anda. Anda akan menanyakan salah satu server ini di langkah berikutnya.

2. Verifikasi bahwa catatan TXT dipublikasikan dengan benar menggunakan perintah berikut, di *name_server* mana salah satu server nama yang Anda temukan di langkah sebelumnya.

```
nslookup -type=TXT _6e86v84tqqubxbwii1m.example.com name_server
```

3. Pada output langkah sebelumnya, verifikasi bahwa string yang mengikuti text = cocok dengan nilai TXT.

Dalam contoh kita, jika catatan dipublikasikan dengan benar, output mencakup yang berikut ini.

```
_6e86v84tqqubxbwii1m.example.com text = "vpce:l6p0ERx1Tt45jevFw0Cp"
```

Memecahkan masalah verifikasi domain

Jika proses verifikasi domain gagal, informasi berikut dapat membantu Anda memecahkan masalah.

- Periksa apakah penyedia DNS Anda mengizinkan garis bawah dalam nama catatan TXT. Jika penyedia DNS Anda tidak mengizinkan garis bawah, Anda dapat menghilangkan nama verifikasi domain (misalnya, “_6e86v84tggqubxbwii1m”) dari catatan TXT.
- Periksa apakah penyedia DNS Anda menambahkan nama domain ke akhir catatan TXT. Beberapa penyedia DNS secara otomatis menambahkan nama domain Anda ke nama atribut dari catatan TXT. Untuk menghindari duplikasi nama domain ini, tambahkan titik di akhir nama domain saat Anda membuat catatan TXT. Ini memberi tahu penyedia DNS Anda bahwa tidak perlu menambahkan nama domain ke catatan TXT.
- Periksa apakah penyedia DNS Anda mengubah nilai catatan DNS untuk hanya menggunakan huruf kecil. Kami memverifikasi domain Anda hanya jika ada catatan verifikasi dengan nilai atribut yang sama persis dengan nilai yang kami berikan. Jika penyedia DNS mengubah nilai catatan TXT Anda untuk hanya menggunakan huruf kecil, hubungi mereka untuk mendapatkan bantuan.
- Anda mungkin perlu memverifikasi domain lebih dari satu kali karena mendukung beberapa Wilayah atau beberapa Akun AWS. Jika penyedia DNS Anda tidak mengizinkan Anda memiliki lebih dari satu catatan TXT dengan nama atribut yang sama, periksa apakah penyedia DNS memungkinkan Anda menetapkan beberapa nilai atribut ke catatan TXT yang sama. Misalnya, jika DNS Anda dikelola oleh Amazon Route 53, Anda dapat menggunakan prosedur berikut.
 1. Di konsol Route 53, pilih catatan TXT yang Anda buat saat memverifikasi domain Anda di Wilayah pertama.
 2. Untuk Nilai, buka akhir nilai atribut yang ada, lalu tekan Enter.
 3. Tambahkan nilai atribut untuk Wilayah tambahan, lalu simpan kumpulan rekaman.

Jika penyedia DNS Anda tidak mengizinkan Anda menetapkan beberapa nilai ke catatan TXT yang sama, Anda dapat memverifikasi domain satu kali dengan nilai dalam nama atribut rekaman TXT, dan sekali lagi dengan nilai yang dihapus dari nama atribut. Namun, Anda hanya dapat memverifikasi domain yang sama dua kali.

Menerima peringatan untuk acara layanan titik akhir

Anda dapat membuat notifikasi untuk menerima peringatan untuk peristiwa tertentu yang terkait dengan layanan titik akhir Anda. Misalnya, Anda dapat menerima email ketika permintaan koneksi diterima atau ditolak.

Tugas

- [Buat notifikasi SNS](#)
- [Menambahkan kebijakan akses](#)
- [Menambahkan kebijakan utama](#)

Buat notifikasi SNS

Gunakan prosedur berikut untuk membuat topik Amazon SNS untuk notifikasi dan berlangganan topik tersebut.

Untuk membuat notifikasi untuk layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Dari tab Notifikasi, pilih Buat notifikasi.
5. Untuk Notifikasi ARN, pilih ARN untuk topik SNS yang Anda buat.
6. Untuk berlangganan acara, pilih dari A cara.
 - Hu bungkan — Konsumen layanan membuat titik akhir antarmuka. Ini mengirimkan permintaan koneksi ke penyedia layanan.
 - Terima — Penyedia layanan menerima permintaan koneksi.
 - Tol ak — Penyedia layanan menolak permintaan koneksi.
 - Hapus — Konsumen layanan menghapus titik akhir antarmuka.
7. Pilih Buat notifikasi.

Untuk membuat notifikasi untuk layanan titik akhir menggunakan baris perintah

- [buat-notifikasi sambungan titik-akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpointConnectionNotification](#)(Alat untuk Windows PowerShell)

Menambahkan kebijakan akses

Tambahkan kebijakan akses ke topik SNS yang memungkinkan AWS PrivateLink untuk mempublikasikan pemberitahuan atas nama Anda, seperti berikut ini. Untuk informasi selengkapnya, lihat [Bagaimana cara mengedit kebijakan akses topik Amazon SNS saya?](#) Gunakan kunci kondisi `aws:SourceArn` dan `aws:SourceAccount` global untuk melindungi dari masalah wakil yang [membingungkan](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "111111111111"
        }
      }
    }
  ]
}
```

Menambahkan kebijakan utama

Jika Anda menggunakan topik SNS terenkripsi, kebijakan sumber daya untuk kunci KMS harus dipercaya untuk memanggil AWS PrivateLink operasi AWS KMS API. Berikut ini adalah contoh kebijakan utama.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "111111111111"
        }
      }
    }
  ]
}
```

Menghapus layanan titik akhir

Ketika Anda selesai dengan layanan endpoint, Anda dapat menghapusnya. Anda tidak dapat menghapus layanan titik akhir jika ada titik akhir yang terhubung ke layanan titik akhir yang berada dalam pending-acceptance status available atau.

Menghapus layanan titik akhir tidak menghapus penyeimbang beban terkait dan tidak memengaruhi server aplikasi yang terdaftar dengan grup target penyeimbang beban.

Untuk menghapus layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.

2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih layanan titik akhir.
4. Pilih Tindakan, Hapus layanan titik akhir.
5. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

Untuk menghapus layanan titik akhir menggunakan baris perintah

- [hapus-konfigurasi layanan-endpoint-vpc-\(\)](#) AWS CLI
- [Remove-EC2EndpointServiceConfiguration](#)(Alat untuk Windows PowerShell)

Akses peralatan virtual melalui AWS PrivateLink

Anda dapat menggunakan Gateway Load Balancer untuk mendistribusikan lalu lintas ke armada peralatan virtual jaringan. Peralatan dapat digunakan untuk inspeksi keamanan, kepatuhan, kontrol kebijakan, dan layanan jaringan lainnya. Anda menentukan Gateway Load Balancer saat membuat layanan titik akhir VPC. Prinsip AWS lainnya mengakses layanan titik akhir dengan membuat titik akhir Gateway Load Balancer.

Harga

Anda ditagih untuk setiap jam titik akhir Gateway Load Balancer disediakan di setiap Zona Ketersediaan. Anda juga ditagih per GB data yang diproses. Untuk informasi selengkapnya, silakan lihat [AWS PrivateLink Harga](#).

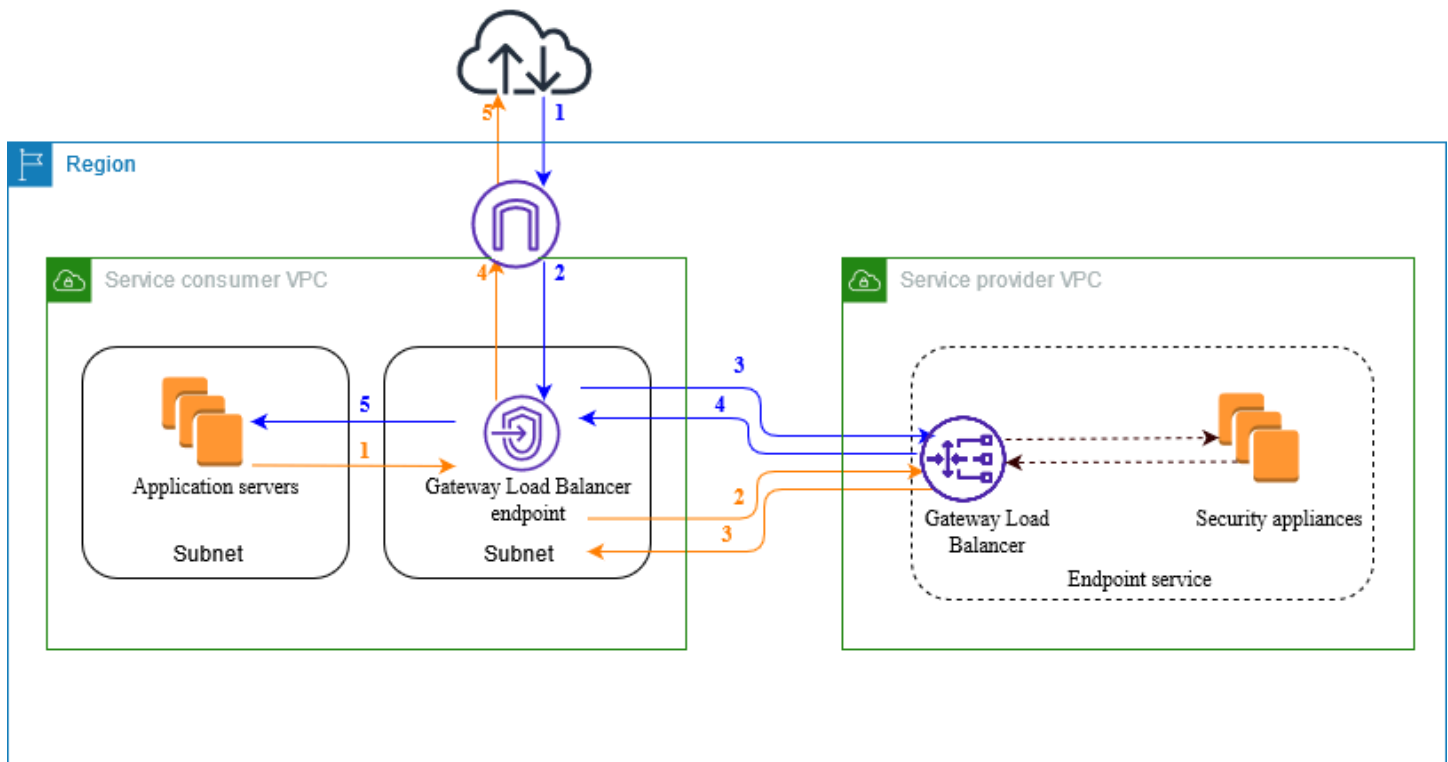
Daftar Isi

- [Gambaran umum](#)
- [Jenis alamat IP](#)
- [Perutean](#)
- [Buat sistem inspeksi sebagai layanan titik akhir Gateway Load Balancer](#)
- [Akses sistem inspeksi menggunakan titik akhir Gateway Load Balancer](#)

Untuk informasi selengkapnya, lihat [Gateway Load Balancers](#).

Gambaran umum

Diagram berikut menunjukkan bagaimana server aplikasi mengakses peralatan keamanan melalui AWS PrivateLink. Server aplikasi berjalan di subnet dari layanan konsumen VPC. Anda membuat titik akhir Gateway Load Balancer di subnet lain dari VPC yang sama. Semua lalu lintas yang memasuki VPC konsumen layanan melalui gateway internet pertama-tama dialihkan ke titik akhir Gateway Load Balancer untuk diperiksa dan kemudian dialihkan ke subnet tujuan. Demikian pula, semua lalu lintas yang meninggalkan server aplikasi dialihkan ke titik akhir Gateway Load Balancer untuk diperiksa sebelum dialihkan kembali melalui gateway internet.



Lalu lintas dari internet ke server aplikasi (panah biru):

1. Lalu lintas memasuki layanan konsumen VPC melalui gateway internet.
2. Lalu lintas dikirim ke titik akhir Gateway Load Balancer, berdasarkan konfigurasi tabel rute.
3. Lalu lintas dikirim ke Gateway Load Balancer untuk diperiksa melalui alat keamanan.
4. Lalu lintas dikirim kembali ke titik akhir Gateway Load Balancer setelah pemeriksaan.
5. Lalu lintas dikirim ke server aplikasi, berdasarkan konfigurasi tabel rute.

Lalu lintas dari server aplikasi ke internet (panah oranye):

1. Lalu lintas dikirim ke titik akhir Gateway Load Balancer, berdasarkan konfigurasi tabel rute.
2. Lalu lintas dikirim ke Gateway Load Balancer untuk diperiksa melalui alat keamanan.
3. Lalu lintas dikirim kembali ke titik akhir Gateway Load Balancer setelah pemeriksaan.
4. Lalu lintas dikirim ke gateway internet berdasarkan konfigurasi tabel rute.
5. Lalu lintas dialihkan kembali ke internet.

Jenis alamat IP

Penyedia layanan dapat membuat titik akhir layanan mereka tersedia untuk konsumen layanan melalui IPv4, IPv6, atau IPv4 dan IPv6, bahkan jika peralatan keamanan mereka hanya mendukung IPv4. Jika Anda mengaktifkan dukungan dualstack, konsumen yang ada dapat terus menggunakan IPv4 untuk mengakses layanan Anda dan konsumen baru dapat memilih untuk menggunakan IPv6 untuk mengakses layanan Anda.

Jika titik akhir Gateway Load Balancer mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir Gateway Load Balancer mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan titik akhir tidak dapat dijangkau dari internet. Jika Anda menjelaskan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Persyaratan untuk mengaktifkan IPv6 untuk layanan titik akhir

- VPC dan subnet untuk layanan endpoint harus memiliki blok IPv6 CIDR terkait.
- Gateway Load Balancer untuk layanan titik akhir harus menggunakan jenis alamat IP dualstack. Peralatan keamanan tidak perlu mendukung lalu lintas IPv6.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir Gateway Load Balancer

- Layanan endpoint harus memiliki tipe alamat IP yang mencakup dukungan IPv6.
- Jenis alamat IP dari titik akhir Gateway Load Balancer harus kompatibel dengan subnet untuk titik akhir Gateway Load Balancer, seperti yang dijelaskan di sini:
 - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
 - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
 - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.
- Tabel rute untuk subnet di VPC konsumen layanan harus merutekan lalu lintas IPv6 dan ACL jaringan untuk subnet ini harus mengizinkan lalu lintas IPv6.

Perutean

Untuk merutekan lalu lintas ke layanan titik akhir, tentukan titik akhir Gateway Load Balancer sebagai target dalam tabel rute Anda, menggunakan ID-nya. Untuk diagram di atas, tambahkan rute ke tabel rute sebagai berikut. Saat menggunakan titik akhir Gateway Load Balancer sebagai target, Anda tidak dapat menentukan daftar awalan sebagai tujuan. Dalam tabel ini, rute IPv6 disertakan untuk konfigurasi dualstack.

Tabel rute untuk gateway internet

Tabel rute ini harus memiliki rute yang mengirimkan lalu lintas yang ditujukan untuk server aplikasi ke titik akhir Gateway Load Balancer.

Tujuan	Target
<i>VPC IPv4 CIDR</i>	Lokal:
<i>VPC IPv6 CIDR</i>	Lokal:
<i>Application subnet IPv4 CIDR</i>	<i>vpc-endpoint-id</i>
<i>Application subnet IPv6 CIDR</i>	<i>vpc-endpoint-id</i>

Tabel rute untuk subnet dengan server aplikasi

Tabel rute ini harus memiliki rute yang mengirimkan semua lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer.

Tujuan	Target
<i>VPC IPv4 CIDR</i>	Lokal:
<i>VPC IPv6 CIDR</i>	Lokal:
0.0.0. 0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

Tabel rute untuk subnet dengan titik akhir Gateway Load Balancer

Tabel rute ini harus mengirim lalu lintas yang dikembalikan dari inspeksi ke tujuan akhirnya. Untuk lalu lintas yang berasal dari internet, rute lokal mengirimkan lalu lintas ke server aplikasi. Untuk lalu lintas yang berasal dari server aplikasi, tambahkan rute yang mengirimkan semua lalu lintas ke gateway internet.

Tujuan	Target
<i>VPC IPv4 CIDR</i>	Lokal:
<i>VPC IPv6 CIDR</i>	Lokal:
0.0.0. 0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Buat sistem inspeksi sebagai layanan titik akhir Gateway Load Balancer

Anda dapat membuat layanan Anda sendiri yang didukung oleh AWS PrivateLink, yang dikenal sebagai layanan titik akhir. Anda adalah penyedia layanan, dan prinsi AWS pal yang membuat koneksi ke layanan Anda adalah konsumen layanan.

Layanan Endpoint memerlukan Network Load Balancer atau Gateway Load Balancer. Dalam hal ini, Anda akan membuat layanan endpoint menggunakan Gateway Load Balancer. Untuk informasi selengkapnya tentang membuat layanan titik akhir menggunakan Network Load Balancer, lihat [Membuat layanan titik akhir](#).

Daftar Isi

- [Pertimbangan-pertimbangan](#)
- [Prasyarat](#)
- [Buat layanan endpoint](#)
- [Jadikan layanan titik akhir Anda tersedia](#)

Pertimbangan-pertimbangan

- Layanan titik akhir tersedia di Wilayah tempat Anda membuatnya.

- Ketika konsumen layanan mengambil informasi tentang layanan titik akhir, mereka hanya dapat melihat Zona Ketersediaan yang mereka miliki bersama dengan penyedia layanan. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Zona Ketersediaan, seperti us-east-1a, mungkin dipetakan ke Zona Ketersediaan fisik yang berbeda di masing-masing Akun AWS. Anda dapat menggunakan ID AZ untuk secara konsisten mengidentifikasi Zona Ketersediaan untuk layanan Anda. Untuk informasi selengkapnya, lihat ID [AZ](#) di Panduan Pengguna Amazon EC2.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat [AWS PrivateLink kuota](#).

Prasyarat

- Buat VPC penyedia layanan dengan setidaknya dua subnet di Zona Ketersediaan tempat layanan harus tersedia. Satu subnet adalah untuk instance alat keamanan dan yang lainnya untuk Gateway Load Balancer.
- Buat Gateway Load Balancer di VPC penyedia layanan Anda. Jika Anda berencana untuk mengaktifkan dukungan IPv6 pada layanan endpoint Anda, Anda harus mengaktifkan dukungan dualstack pada Gateway Load Balancer. Untuk informasi selengkapnya, lihat [Memulai dengan Gateway Load Balancers](#).
- Luncurkan peralatan keamanan di VPC penyedia layanan dan daftarkan mereka dengan kelompok target penyeimbang beban.

Buat layanan endpoint

Gunakan prosedur berikut untuk membuat layanan titik akhir menggunakan Gateway Load Balancer.

Untuk membuat layanan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih layanan Endpoint.
3. Pilih Buat layanan titik akhir.
4. Untuk jenis penyeimbang beban, pilih Gateway.
5. Untuk penyeimbang beban yang tersedia, pilih Gateway Load Balancer Anda.

6. Untuk Memerlukan penerimaan untuk titik akhir, pilih Penerimaan diperlukan untuk mengharuskan permintaan koneksi ke layanan titik akhir Anda diterima secara manual. Jika tidak, mereka diterima secara otomatis.
7. Untuk jenis alamat IP yang didukung, lakukan salah satu hal berikut:
 - Pilih IPv4 — Aktifkan layanan titik akhir untuk menerima permintaan IPv4.
 - Pilih IPv6 — Aktifkan layanan titik akhir untuk menerima permintaan IPv6.
 - Pilih IPv4 dan IPv6 — Aktifkan layanan titik akhir untuk menerima permintaan IPv4 dan IPv6.
8. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
9. Pilih Buat.

Untuk membuat layanan titik akhir menggunakan baris perintah

- [buat-konfigurasi layanan-endpoint-vpc-\(\)](#) AWS CLI
- [New-EC2VpcEndpointServiceConfiguration](#)(Alat untuk Windows PowerShell)

Jadikan layanan titik akhir Anda tersedia

Penyedia layanan harus melakukan hal berikut untuk membuat layanan mereka tersedia bagi konsumen layanan.

- Tambahkan izin yang memungkinkan setiap konsumen layanan terhubung ke layanan titik akhir Anda. Untuk informasi selengkapnya, lihat [the section called “Kelola izin”](#).
- Berikan nama layanan Anda dan Zona Ketersediaan yang didukung kepada konsumen layanan sehingga mereka dapat membuat titik akhir antarmuka untuk terhubung ke layanan Anda. Untuk informasi lebih lanjut, lihat prosedur di bawah ini.
- Terima permintaan koneksi titik akhir dari konsumen layanan. Untuk mengetahui informasi selengkapnya, lihat [the section called “Menerima atau tolak permintaan koneksi”](#).

AWS prinsipal dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir Gateway Load Balancer. Untuk informasi selengkapnya, lihat [Membuat titik akhir Gateway Load Balancer](#).

Akses sistem inspeksi menggunakan titik akhir Gateway Load Balancer

Anda dapat membuat titik akhir Gateway Load Balancer untuk terhubung ke layanan [titik akhir yang](#) didukung oleh AWS PrivateLink.

Untuk setiap subnet yang Anda tentukan dari VPC Anda, kami membuat antarmuka jaringan titik akhir di subnet dan menetapkan alamat IP pribadi dari rentang alamat subnet. Antarmuka jaringan titik akhir adalah antarmuka jaringan yang dikelola permintaan; Anda dapat melihatnya di Akun AWS, tetapi Anda tidak dapat mengelolanya sendiri.

Anda ditagih untuk biaya penggunaan dan pemrosesan data per jam. Untuk informasi selengkapnya, lihat Harga titik akhir [Gateway Load Balancer](#).

Daftar Isi

- [Pertimbangan-pertimbangan](#)
- [Prasyarat](#)
- [Buat titik akhir](#)
- [Konfigurasi perutean](#)
- [Kelola tanda](#)
- [Menghapus titik akhir Gateway Load Balancer](#)

Pertimbangan-pertimbangan

- Anda hanya dapat memilih satu Zona Ketersediaan di VPC konsumen layanan. Anda tidak dapat mengubah subnet ini nanti. Untuk menggunakan titik akhir Gateway Load Balancer di subnet yang berbeda, Anda harus membuat titik akhir Gateway Load Balancer baru.
- Anda dapat membuat satu titik akhir Gateway Load Balancer per Availability Zone per layanan, dan Anda harus memilih Availability Zone yang didukung Gateway Load Balancer. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Zona Ketersediaan, seperti us-east-1a, mungkin dipetakan ke Zona Ketersediaan fisik yang berbeda di masing-masing Akun AWS. Anda dapat menggunakan ID AZ untuk secara konsisten mengidentifikasi Zona Ketersediaan untuk layanan Anda. Untuk informasi selengkapnya, lihat ID [AZ](#) di Panduan Pengguna Amazon EC2.

- Sebelum Anda dapat menggunakan layanan titik akhir, penyedia layanan harus menerima permintaan koneksi. Layanan tidak dapat memulai permintaan ke sumber daya di VPC Anda melalui titik akhir VPC. Titik akhir hanya mengembalikan respons terhadap lalu lintas yang dimulai oleh sumber daya di VPC Anda.
- Setiap titik akhir Gateway Load Balancer dapat mendukung bandwidth hingga 10 Gbps per Availability Zone dan secara otomatis menskalakan hingga 100 Gbps.
- Jika layanan titik akhir dikaitkan dengan beberapa Gateway Load Balancers, titik akhir Gateway Load Balancer membuat koneksi dengan hanya satu penyeimbang beban per Availability Zone.
- Untuk menjaga lalu lintas dalam Zona Ketersediaan yang sama, sebaiknya buat titik akhir Gateway Load Balancer di setiap Zona Ketersediaan tempat Anda akan mengirim lalu lintas.
- Pelestarian IP klien Network Load Balancer tidak didukung saat lalu lintas dialihkan melalui titik akhir Gateway Load Balancer, bahkan jika target berada di VPC yang sama dengan Network Load Balancer.
- Jika server aplikasi dan titik akhir Gateway Load Balancer berada di subnet yang sama, aturan NACL dievaluasi untuk lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer.
- Jika Anda menggunakan Gateway Load Balancer dengan gateway internet khusus egress, lalu lintas IPv6 akan dihapus. Sebagai gantinya, gunakan gateway internet dan aturan firewall masuk.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat [AWS PrivateLink kuota](#).

Prasyarat

- Buat VPC konsumen layanan dengan setidaknya dua subnet di Zona Ketersediaan tempat Anda akan mengakses layanan. Satu subnet adalah untuk server aplikasi dan yang lainnya adalah untuk titik akhir Gateway Load Balancer.
- Untuk memverifikasi Zona Ketersediaan mana yang didukung oleh layanan titik akhir, jelaskan layanan titik akhir menggunakan konsol atau perintah [describe-v](#) pc-endpoint-services.
- Jika sumber daya Anda berada di subnet dengan ACL jaringan, verifikasi bahwa ACL jaringan memungkinkan lalu lintas antara antarmuka jaringan titik akhir dan sumber daya di VPC.

Buat titik akhir

Gunakan prosedur berikut untuk membuat titik akhir Gateway Load Balancer yang terhubung ke layanan titik akhir untuk sistem inspeksi.

Untuk membuat titik akhir Gateway Load Balancer menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih layanan Endpoint yang menggunakan NLB dan GW LB.
5. Untuk Nama layanan, masukkan nama layanan, lalu pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC tempat Anda akan mengakses layanan titik akhir.
7. Untuk Subnet, pilih satu subnet untuk membuat antarmuka jaringan titik akhir.
8. Untuk jenis alamat IP, pilih dari opsi berikut:
 - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika subnet yang dipilih memiliki rentang alamat IPv4.
 - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika subnet yang dipilih adalah subnet khusus IPv6.
 - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.
9. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
10. Pilih Buat titik akhir. Status awal adalah pending acceptance.

Untuk membuat titik akhir Gateway Load Balancer menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Konfigurasi perutean

Gunakan prosedur berikut untuk mengonfigurasi tabel rute untuk VPC konsumen layanan. Hal ini memungkinkan peralatan keamanan untuk melakukan pemeriksaan keamanan untuk lalu lintas masuk yang ditujukan untuk server aplikasi. Untuk informasi selengkapnya, lihat [the section called "Perutean"](#).

Untuk mengkonfigurasi routing menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Tabel Route.
3. Pilih tabel rute untuk gateway internet dan lakukan hal berikut:
 - a. Pilih Tindakan, Sunting rute.
 - b. Jika Anda mendukung IPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan blok IPv4 CIDR subnet untuk server aplikasi. Untuk Target, pilih titik akhir VPC.
 - c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan blok IPv6 CIDR subnet untuk server aplikasi. Untuk Target, pilih titik akhir VPC.
 - d. Pilih Simpan perubahan.
4. Pilih tabel rute untuk subnet dengan server aplikasi dan lakukan hal berikut:
 - a. Pilih Tindakan, Sunting rute.
 - b. Jika Anda mendukung IPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan **0.0.0.0/0**. Untuk Target, pilih titik akhir VPC.
 - c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan **::/0**. Untuk Target, pilih titik akhir VPC.
 - d. Pilih Simpan perubahan.
5. Pilih tabel rute untuk subnet dengan titik akhir Gateway Load Balancer, dan lakukan hal berikut:
 - a. Pilih Tindakan, Sunting rute.
 - b. Jika Anda mendukung IPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan **0.0.0.0/0**. Untuk Target, pilih gateway internet.
 - c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan **::/0**. Untuk Target, pilih gateway internet.
 - d. Pilih Simpan perubahan.

Untuk mengkonfigurasi routing menggunakan baris perintah

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (Alat untuk Windows PowerShell)

Kelola tanda

Anda dapat menandai titik akhir Gateway Load Balancer untuk membantu mengidentifikasi atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk mengelola tag menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag yang akan ditambahkan pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag menggunakan baris perintah

- [buat-tag](#) dan hapus tag ([AWS CLI](#))
- [New-EC2Tag](#) dan [Remove-EC2Tag](#) (Alat untuk Windows PowerShell)

Menghapus titik akhir Gateway Load Balancer

Ketika Anda selesai dengan titik akhir, Anda dapat menghapusnya. Menghapus titik akhir Gateway Load Balancer juga menghapus antarmuka jaringan titik akhir. Anda tidak dapat menghapus titik akhir Gateway Load Balancer jika ada rute di tabel rute yang mengarah ke titik akhir.

Untuk menghapus titik akhir Gateway Load Balancer

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik Akhir dan pilih titik akhir Anda.
3. Pilih Tindakan, Hapus Titik Akhir.
4. Di layar konfirmasi, pilih Ya, Hapus.

Untuk menghapus titik akhir Gateway Load Balancer

- [hapus titik akhir vpc \(\)](#) AWS CLI
- [Remove-EC2VpcEndpoint](#) (AWS Tools for Windows PowerShell)

Akses sumber daya VPC melalui AWS PrivateLink

Anda dapat mengakses sumber daya VPC secara pribadi di VPC lain menggunakan titik akhir VPC sumber daya (titik akhir sumber daya). Titik akhir sumber daya memungkinkan Anda mengakses sumber daya VPC secara pribadi dan aman seperti database, instans Amazon EC2, titik akhir aplikasi, target nama domain, atau alamat IP yang mungkin berada di subnet pribadi di VPC lain atau di lingkungan lokal. Tanpa titik akhir sumber daya, Anda harus menambahkan gateway internet ke VPC Anda atau mengakses sumber daya menggunakan titik akhir AWS PrivateLink antarmuka dan Network Load Balancer. Titik akhir sumber daya tidak memerlukan penyeimbang [bang beban](#), sehingga Anda dapat mengakses sumber daya VPC secara langsung. Sumber daya VPC diwakili oleh konfigurasi sumber daya. Konfigurasi sumber daya dikaitkan dengan gateway sumber daya.

Harga

Saat Anda mengakses sumber daya menggunakan titik akhir sumber daya, Anda ditagih untuk setiap jam titik akhir VPC sumber daya Anda disediakan. Anda juga ditagih per GB data yang diproses saat mengakses sumber daya. Untuk informasi selengkapnya, lihat [harga AWS PrivateLink](#). Saat Anda mengaktifkan akses ke sumber daya menggunakan konfigurasi sumber daya dan gateway sumber daya, Anda ditagih per GB data yang diproses oleh gateway sumber daya Anda. Untuk informasi selengkapnya, lihat [harga Amazon VPC Lattice](#).

Daftar Isi

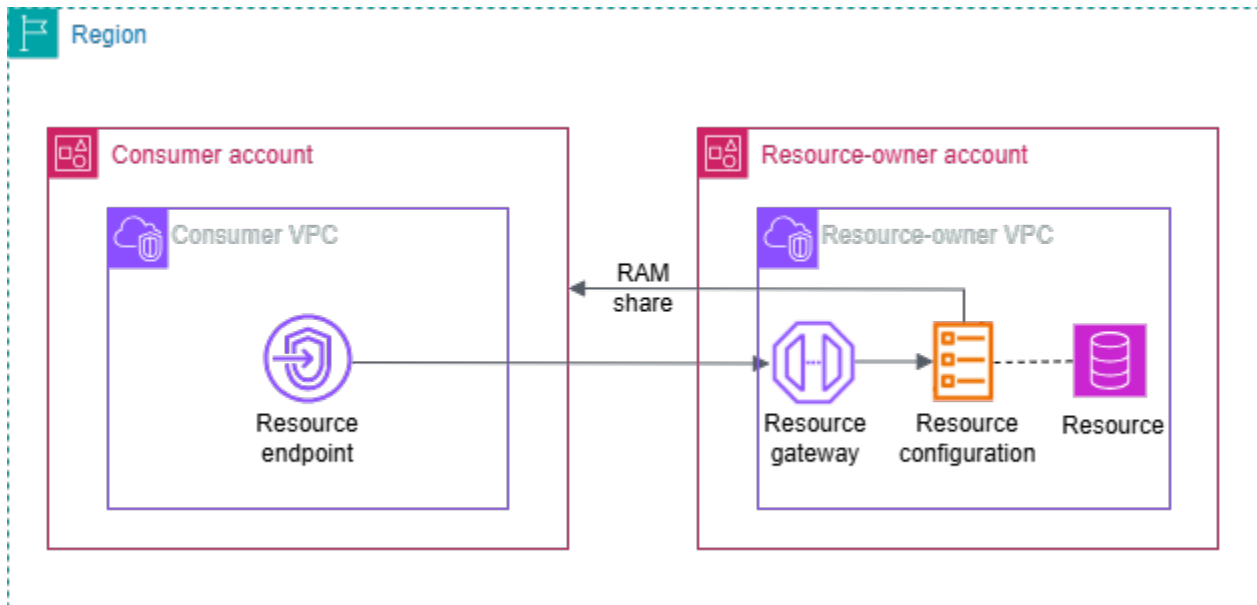
- [Gambaran umum](#)
- [Nama host DNS](#)
- [Resolusi DNS](#)
- [DNS privat](#)
- [Subnet dan Zona Ketersediaan](#)
- [Jenis alamat IP](#)
- [Mengakses sumber daya melalui titik akhir VPC sumber daya](#)
- [Kelola titik akhir sumber daya](#)

Gambaran umum

Anda dapat mengakses sumber daya di akun Anda atau yang telah dibagikan dengan Anda dari akun lain. Untuk mengakses sumber daya, Anda membuat titik akhir VPC sumber daya, yang membuat

koneksi antara subnet di VPC Anda dan sumber daya menggunakan antarmuka jaringan. Lalu lintas yang ditujukan untuk sumber daya diselesaikan ke alamat IP pribadi dari antarmuka jaringan titik akhir sumber daya menggunakan DNS. Kemudian, lalu lintas dikirim ke sumber daya menggunakan koneksi antara titik akhir VPC dan sumber daya melalui gateway sumber daya.

Gambar berikut menunjukkan titik akhir sumber daya di akun konsumen yang mengakses sumber daya yang dimiliki oleh akun lain dan dibagikan melalui AWS RAM:



Pertimbangan-pertimbangan

- Lalu lintas TCP didukung. Lalu lintas UDP tidak didukung.
- Koneksi jaringan harus dimulai dari VPC yang berisi titik akhir sumber daya, dan bukan dari VPC yang memiliki sumber daya. VPC sumber daya tidak dapat memulai koneksi jaringan ke VPC titik akhir.
- Satu-satunya ARN-based sumber daya yang didukung adalah sumber daya Amazon RDS.
- Setidaknya satu Zona [Ketersediaan](#) dari titik akhir VPC dan gateway sumber daya harus tumpang tindih.

Nama host DNS

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke sumber daya menggunakan titik akhir pribadi. Saat Anda membuat titik akhir VPC sumber daya, kami membuat nama DNS Regional (disebut nama DNS default) yang dapat Anda gunakan untuk berkomunikasi dengan sumber daya dari VPC Anda

dan dari lokasi. Sebaiknya gunakan DNS alih-alih IP titik akhir untuk menyambung ke sumber daya Anda. Nama DNS default untuk titik akhir VPC sumber daya Anda memiliki sintaks berikut:

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Saat Anda membuat titik akhir VPC sumber daya untuk konfigurasi sumber daya tertentu yang menggunakan ARN, Anda dapat mengaktifkan DNS [pribadi](#). Dengan DNS pribadi, Anda dapat terus membuat permintaan ke sumber daya menggunakan nama DNS yang disediakan untuk sumber daya oleh AWS layanan, sambil memanfaatkan konektivitas pribadi melalui titik akhir VPC sumber daya. Untuk informasi selengkapnya, lihat [the section called “Resolusi DNS”](#).

Perintah [describe-vpc-endpoint-association](#) berikut menampilkan entri DNS untuk titik akhir sumber daya.

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].*'
```

Berikut ini adalah contoh output untuk titik akhir sumber daya untuk database Amazon RDS dengan nama DNS pribadi diaktifkan. Nama DNS pertama adalah nama DNS default. Nama DNS kedua berasal dari zona host pribadi tersembunyi, yang menyelesaikan permintaan ke titik akhir publik ke alamat IP pribadi dari antarmuka jaringan titik akhir.

```
[
  [
    "vpce-rsc-asc-abcd1234abcd",
    "vpce-123456789abcdefgh",
    "Accessible",
    {
      "DnsName": "vpce-1234567890abcdefgh-
snra-1234567890abcdefgh.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
      "HostedZoneId": "ABCDEFGH123456789000"
    },
    {
      "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
      "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
    },
    "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890abcdefgh",
```

```
"arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890xyz"
]
]
```

Resolusi DNS

Catatan DNS yang kami buat untuk titik akhir VPC sumber daya Anda bersifat publik. Oleh karena itu, nama-nama DNS ini dapat diselesaikan secara publik. Namun, permintaan DNS dari luar VPC masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir sumber daya. Anda dapat menggunakan nama DNS ini untuk mengakses sumber daya dari lokasi, selama Anda memiliki akses ke VPC tempat titik akhir sumber daya berada, melalui VPN atau Direct Connect.

DNS privat

Jika Anda mengaktifkan DNS pribadi untuk titik akhir VPC sumber daya untuk konfigurasi sumber daya tertentu yang menggunakan ARN, dan VPC Anda [mengaktifkan nama host](#) DNS dan resolusi DNS, kami membuat zona host pribadi tersembunyi yang AWS dikelola untuk konfigurasi sumber daya dengan nama DNS khusus. Zona yang dihosting berisi kumpulan rekaman untuk nama DNS default untuk sumber daya yang menyelesaikannya ke alamat IP pribadi antarmuka jaringan titik akhir sumber daya di VPC Anda.

Amazon menyediakan server DNS untuk VPC Anda, yang disebut [Route 53 Resol](#) ver. Route 53 Resolver secara otomatis menyelesaikan nama domain VPC lokal dan rekaman di zona yang dihosting pribadi. Namun, Anda tidak dapat menggunakan Route 53 Resolver dari luar VPC Anda. Jika Anda ingin mengakses titik akhir VPC dari jaringan lokal, Anda dapat menggunakan nama DNS khusus atau Anda dapat menggunakan titik akhir Resolver Route 53 dan aturan Resolver. Untuk informasi selengkapnya, lihat [Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver](#).

Subnet dan Zona Ketersediaan

Anda dapat mengonfigurasi titik akhir VPC Anda dengan satu subnet per Zona Ketersediaan. Kami membuat antarmuka jaringan titik akhir untuk titik akhir VPC di subnet Anda. Kami menetapkan alamat IP ke setiap antarmuka jaringan titik akhir dari subnetnya, berdasarkan jenis alamat [IP](#) dari titik akhir VPC. Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, sebaiknya konfigurasi setidaknya dua Zona Ketersediaan untuk setiap titik akhir VPC.

Jenis alamat IP

Titik akhir sumber daya dapat mendukung alamat IPv4, IPv6, atau dualstack. Endpoint yang mendukung IPv6 dapat menanggapi kueri DNS dengan catatan AAAA. Jenis alamat IP dari titik akhir sumber daya harus kompatibel dengan subnet untuk titik akhir sumber daya, seperti yang dijelaskan di sini:

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

Jika titik akhir VPC sumber daya mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir VPC sumber daya mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan titik akhir tidak dapat dijangkau dari internet. Jika Anda menjelaskan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Mengakses sumber daya melalui titik akhir VPC sumber daya

Anda dapat mengakses sumber daya VPC seperti nama domain, alamat IP, atau database Amazon RDS menggunakan titik akhir sumber daya. Titik akhir sumber daya menyediakan akses pribadi ke sumber daya. Saat Anda membuat titik akhir sumber daya, Anda menentukan konfigurasi sumber daya tipe tunggal, grup, atau ARN. Titik akhir sumber daya dapat dikaitkan dengan hanya satu konfigurasi sumber daya. Konfigurasi sumber daya dapat mewakili sumber daya tunggal atau sekelompok sumber daya.

Prasyarat

Untuk membuat titik akhir sumber daya, Anda harus memenuhi prasyarat berikut.

- Anda harus memiliki konfigurasi sumber daya yang Anda buat atau akun lain yang dibuat dan dibagikan dengan Anda AWS RAM.

- Jika konfigurasi sumber daya dibagikan dengan Anda dari akun lain, Anda harus meninjau dan menerima pembagian sumber daya yang berisi konfigurasi sumber daya. Untuk informasi selengkapnya, [lihat Menerima dan menolak undangan](#) di Panduan AWS RAM Pengguna.

VPC Lattice tidak membuat titik akhir sumber daya jika berikut ini benar:

- Gateway sumber daya berada di VPC yang sama dengan titik akhir sumber daya.
- Untuk target nama domain
 - Resolusi DNS diatur ke IN_VPC pada gateway sumber daya.
 - Nama domain kustom atau domain grup adalah domain tingkat yang sama atau lebih tinggi dari target nama domain.

Membuat titik akhir sumber daya VPC

Gunakan prosedur berikut untuk membuat titik akhir sumber daya VPC. Setelah Anda membuat titik akhir sumber daya, Anda hanya dapat mengubah grup atau tag keamanannya.

Untuk membuat titik akhir sumber daya VPC

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Anda dapat menentukan nama untuk membuatnya lebih mudah untuk menemukan dan mengelola titik akhir.
5. Untuk Jenis, pilih Sumber Daya.
6. Untuk konfigurasi sumber daya, pilih konfigurasi sumber daya.
7. Untuk Pengaturan jaringan, pilih VPC tempat Anda akan mengakses sumber daya.
8. Jika, Anda ingin mengonfigurasi dukungan DNS pribadi untuk konfigurasi sumber daya, pilih Pengaturan tambahan, Aktifkan nama DNS. Untuk menggunakan fitur ini, pastikan atribut Aktifkan nama host DNS dan Aktifkan dukungan DNS diaktifkan untuk VPC Anda. Untuk informasi selengkapnya, lihat [the section called “Nama domain khusus untuk konsumen sumber daya”](#).
9. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir.

Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, sebaiknya konfigurasi setidaknya dua Zona Ketersediaan untuk setiap titik akhir VPC.

10. Untuk Grup keamanan, pilih grup keamanan.

Jika Anda tidak menentukan grup keamanan, kami mengaitkan grup keamanan default untuk VPC.

11. Pilih Buat titik akhir.

Untuk membuat titik akhir sumber daya menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Kelola titik akhir sumber daya

Setelah membuat titik akhir sumber daya, Anda dapat mengelola grup atau tag keamanannya.

Tugas

- [Hapus titik akhir](#)
- [Memperbarui titik akhir](#)

Hapus titik akhir

Setelah selesai dengan titik akhir VPC, Anda dapat menghapusnya.

Untuk menghapus titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir menggunakan baris perintah

- [hapus titik akhir vpc \(\)](#) AWS CLI
- [Remove-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Memperbarui titik akhir

Anda dapat memperbarui titik akhir VPC.

Untuk memperbarui titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, dan opsi yang sesuai.
5. Ikuti langkah-langkah konsol untuk mengirimkan pembaruan.

Untuk memperbarui titik akhir menggunakan baris perintah

- [modify-vpc-endpoint \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Akses segmen jaringan melalui AWS PrivateLink

Anda dapat mengakses segmen jaringan secara pribadi di VPC lain menggunakan titik akhir VPC terowongan (titik akhir terowongan). Titik akhir terowongan memungkinkan Anda mengakses sumber daya secara pribadi dan aman yang terletak dalam serangkaian rentang CIDR di jaringan lain. Rentang CIDR mewakili segmen jaringan, sehingga aplikasi konsumen dapat menjangkau sumber daya apa pun dalam segmen jaringan itu, tanpa penyedia harus menghitung setiap sumber daya. Ini berguna ketika sumber daya fana atau tidak diketahui sebelumnya. Titik akhir terowongan mengharuskan Anda untuk membuat terowongan ke VPC lain menggunakan enkapsulasi GENEVE.

Harga

Saat Anda mengakses segmen jaringan menggunakan titik akhir terowongan, Anda akan ditagih untuk setiap jam penyediaan titik akhir terowongan. Anda juga ditagih per GB data yang diproses saat mengakses segmen jaringan. Untuk informasi selengkapnya, lihat [harga AWS PrivateLink](#). Saat berbagi segmen jaringan menggunakan konfigurasi sumber daya dan gateway sumber daya, Anda ditagih per GB data yang diproses oleh gateway sumber daya Anda. Untuk informasi selengkapnya, lihat [harga Amazon VPC Lattice](#).

Daftar Isi

- [Gambaran umum](#)
- [Geneve enkapsulasi](#)
- [Nama host DNS](#)
- [Resolusi DNS](#)
- [DNS privat](#)
- [Subnet dan Zona Ketersediaan](#)
- [Jenis alamat IP](#)
- [Akses segmen jaringan melalui titik akhir VPC terowongan](#)

Gambaran umum

Anda dapat mengakses segmen jaringan di akun Anda atau yang telah dibagikan dengan Anda dari akun lain. Untuk mengakses segmen jaringan, pertama-tama Anda membuat titik akhir terowongan, yang membuat koneksi antara VPC Anda dan gateway sumber daya di VPC tempat segmen

jaringan dibagikan. Anda kemudian merangkum lalu lintas aplikasi menggunakan GENEVE dan mengirimkannya ke titik akhir terowongan. Titik akhir menghapus header GENEVE dan mengirimkan paket dalam ke tujuannya di VPC lainnya. Saat melakukannya, ia memeriksa apakah tujuan terletak di dalam segmen jaringan yang dibagikan dengan Anda dari VPC lain. Jika terletak di luar, titik akhir tidak mengizinkan akses ke sana.

Pertimbangan-pertimbangan

- Subnet dari titik akhir terowongan harus tumpang tindih dengan subnet tempat gateway sumber daya berada. Zona Ketersediaan Zona Ketersediaan
- Koneksi jaringan hanya dapat dimulai dari VPC yang memiliki titik akhir terowongan, dan bukan VPC yang berbagi segmen jaringan. Segmen jaringan VPC tidak dapat memulai koneksi jaringan ke titik akhir VPC.

Geneve enkapsulasi

Lalu lintas aplikasi harus dienkapsulasi dalam GENEVE. Lalu lintas GENEVE harus menggunakan UDP dan port 6081 pada titik akhir terowongan. VNI harus diatur ke 0. Paket bagian dalam harus berupa paket IP layer 3. Dalam paket bagian dalam, UDP hanya didukung untuk kueri DNS. Lalu lintas aplikasi reguler di paket dalam harus TCP.

Nama host DNS

Titik akhir terowongan memiliki nama DNS regional. Ini diselesaikan ke IP di subnet tempat titik akhir terowongan dibuat. IP ini harus menjadi target GENEVE-encapsulated lalu lintas Anda, bukan lalu lintas aplikasi. Nama DNS pribadi tidak didukung untuk titik akhir terowongan.

Resolusi DNS

Titik akhir terowongan memungkinkan Anda menyelesaikan DNS dalam konteks VPC yang berbagi segmen jaringan. Anda dapat menyelesaikan domain melalui titik akhir terowongan terhadap resolver DNS dari VPC jarak jauh. Untuk melakukannya, Anda gunakan 169.254.168.253 sebagai server nama. Anda mengaturnya sebagai tujuan kueri DNS di paket dalam, dan merangkumnya di GENEVE seperti yang Anda lakukan untuk lalu lintas aplikasi. Resolusi DNS terlihat sama seperti untuk klien di VPC jarak jauh. Ini didasarkan pada set opsi DHCP yang dikonfigurasi VPC jarak jauh. Ini menghormati zona host pribadi Route 53 atau resolver khusus yang dikonfigurasi di VPC jarak jauh.

DNS privat

Nama DNS pribadi tidak didukung untuk titik akhir terowongan.

Subnet dan Zona Ketersediaan

Anda dapat mengonfigurasi titik akhir terowongan dengan satu subnet per Zona Ketersediaan. Antarmuka jaringan elastis dibuat untuk titik akhir di subnet tersebut. Alamat IP ditetapkan untuk setiap ENI dari subnetnya, berdasarkan jenis alamat IP dari titik akhir. Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, sebaiknya konfigurasi setidaknya dua Zona Ketersediaan untuk setiap titik akhir. Subnet titik akhir harus tumpang tindih dengan subnet tempat gateway sumber daya berada. Zona Ketersediaan Zona Ketersediaan

Jenis alamat IP

Paket luar dan dalam dapat memiliki tipe IP yang berbeda. Kombinasi berikut didukung: IPv4 melalui IPv4, IPv6 melalui IPv4, IPv4 melalui IPv6, dan IPv6 melalui IPv6.

Tipe IP titik akhir terowongan menentukan jenis IP dari paket GENEVE luar. Jenis IP VPC jarak jauh menentukan jenis IP paket dalam. Segmen jaringan yang dibagikan dapat memiliki rentang IPv4 dan IPv6.

Titik akhir terowongan mendukung alamat IPv4, IPv6, atau dualstack. Jenis alamat IP dari titik akhir terowongan harus kompatibel dengan subnet untuk titik akhir terowongan, seperti yang dijelaskan di sini:

- IPv4 — Menetapkan alamat IPv4 ke titik akhir terowongan. Didukung hanya jika semua subnet titik akhir memiliki rentang IPv4.
- IPv6 — Menetapkan alamat IPv6 ke titik akhir terowongan. Didukung hanya jika semua subnet titik akhir memiliki rentang IPv6.
- Dualstack — Menetapkan alamat IPv4 dan IPv6 ke titik akhir terowongan. Didukung hanya jika semua subnet titik akhir memiliki rentang IPv4 dan IPv6.

Alamat IPv6 endpoint tidak dapat dijangkau dari internet. `denyAllIgwTraffic` diaktifkan pada antarmuka jaringannya.

Akses segmen jaringan melalui titik akhir VPC terowongan

Anda dapat mengakses segmen jaringan melalui titik akhir terowongan. Segmen jaringan adalah sekumpulan rentang CIDR. Ini dibagikan sebagai konfigurasi sumber daya tipe CIDR. Titik akhir terowongan dikaitkan dengan persis satu konfigurasi CIDR-type sumber daya.

Prasyarat

Untuk membuat titik akhir terowongan, Anda harus memenuhi prasyarat berikut.

- Anda harus memiliki konfigurasi CIDR-type sumber daya yang Anda buat, atau akun lain yang dibuat dan dibagikan dengan Anda AWS RAM.
- Jika konfigurasi sumber daya dibagikan dengan Anda dari akun lain, Anda harus meninjau dan menerima pembagian sumber daya yang berisi konfigurasi sumber daya. Untuk informasi selengkapnya, [lihat Menerima dan menolak undangan](#) di Panduan AWS RAM Pengguna.
- Konfigurasi sumber daya harus dilampirkan ke gateway sumber daya yang bendera resolusi DNS-nya diatur keIN_VPC.
- VPC konsumen Anda harus memiliki subnet Zona Ketersediaan yang tumpang tindih dengan gateway sumber daya penyedia. Zona Ketersediaan
- Komputasi konsumen Anda harus dapat merangkum lalu lintas aplikasi di GENEVE. VNI harus diatur ke0. Paket bagian dalam harus berupa paket IP layer 3. Ini idealnya harus dilakukan dalam konteks routing atau namespace jaringan sendiri.
- Grup keamanan pada titik akhir dan komputasi harus mengizinkan port UDP 6081.

Membuat titik akhir VPC terowongan

Setelah membuat titik akhir terowongan, Anda harus menjelaskan hubungannya untuk mendapatkan alamat IP titik akhir Zona ketersediaan per ketersediaan, lalu mengonfigurasi perangkat GENEVE dan server nama terowongan pada komputasi Anda.

Untuk membuat titik akhir terowongan (konsol)

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. (Opsional) Masukkan nama untuk memudahkan menemukan dan mengelola titik akhir.

5. Untuk Jenis, pilih tipe titik akhir terowongan.
6. Untuk konfigurasi sumber daya, pilih konfigurasi sumber daya CIDR.
7. Untuk pengaturan Jaringan, pilih VPC tempat Anda akan mengakses jangkauan.
8. Untuk Subnet, pilih subnet di setiap Zona Ketersediaan yang tumpang tindih dengan gateway sumber daya. Zona Ketersediaan
9. Untuk Grup keamanan, pilih grup keamanan yang mengizinkan port UDP 6081. Jika Anda tidak menentukan grup keamanan, kami mengaitkan grup keamanan default untuk VPC.
10. Pilih Buat titik akhir.

Perintah [create-vpc-endpoint](#) berikut membuat titik akhir terowongan untuk konfigurasi sumber daya CIDR:

```
aws ec2 create-vpc-endpoint \  
  --vpc-endpoint-type Tunnel \  
  --vpc-id vpc-1a2b3c4d \  
  --subnet-ids subnet-1a2b3c4d \  
  --ip-address-type ipv4 \  
  --resource-configuration-arn arn:aws:vpc-lattice:us-  
east-1:111122223333:resourceconfiguration/rcfg-1234567890abcdefg
```

Untuk membuat titik akhir terowongan menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Akses jaringan layanan melalui AWS PrivateLink

Anda dapat terhubung secara pribadi ke jaringan layanan dari VPC menggunakan titik akhir VPC jaringan layanan (titik akhir jaringan layanan). Titik akhir jaringan layanan memungkinkan Anda mengakses sumber daya dan layanan yang terkait dengan jaringan layanan secara pribadi dan aman. Dengan cara ini, Anda dapat mengakses beberapa sumber daya dan layanan secara pribadi melalui satu titik akhir VPC.

Jaringan layanan adalah kumpulan logis konfigurasi sumber daya dan layanan VPC Lattice. Menggunakan titik akhir jaringan layanan, Anda dapat menghubungkan jaringan layanan ke VPC Anda, dan mengakses sumber daya dan layanan tersebut secara pribadi dari VPC Anda atau dari lokal. Titik akhir jaringan layanan memungkinkan Anda terhubung ke satu jaringan layanan. Untuk menyambung ke beberapa jaringan layanan dari VPC Anda, Anda dapat membuat beberapa titik akhir jaringan layanan, masing-masing menunjuk ke jaringan layanan yang berbeda.

Jaringan layanan terintegrasi dengan AWS Resource Access Manager (AWS RAM). Anda dapat berbagi jaringan layanan Anda dengan akun lain melalui AWS RAM. Saat Anda berbagi jaringan layanan dengan AWS akun lain, akun tersebut dapat membuat titik akhir jaringan layanan untuk terhubung ke jaringan layanan. Anda dapat berbagi jaringan layanan menggunakan berbagi [sumber daya](#) di AWS RAM.

Gunakan AWS RAM konsol, untuk melihat berbagi sumber daya yang telah ditambahkan, jaringan layanan bersama yang dapat Anda akses, dan AWS akun yang telah berbagi sumber daya dengan Anda. Untuk informasi selengkapnya, lihat [Sumber daya yang dibagikan dengan Anda](#) di Panduan AWS RAM Pengguna.

Harga

Anda ditagih per jam untuk konfigurasi sumber daya yang terkait dengan jaringan layanan Anda. Anda juga ditagih per GB data yang diproses saat mengakses sumber daya melalui titik akhir VPC jaringan layanan. Anda tidak ditagih per jam untuk titik akhir VPC jaringan layanan itu sendiri. Untuk informasi selengkapnya, lihat [harga Amazon VPC Lattice](#).

Daftar Isi

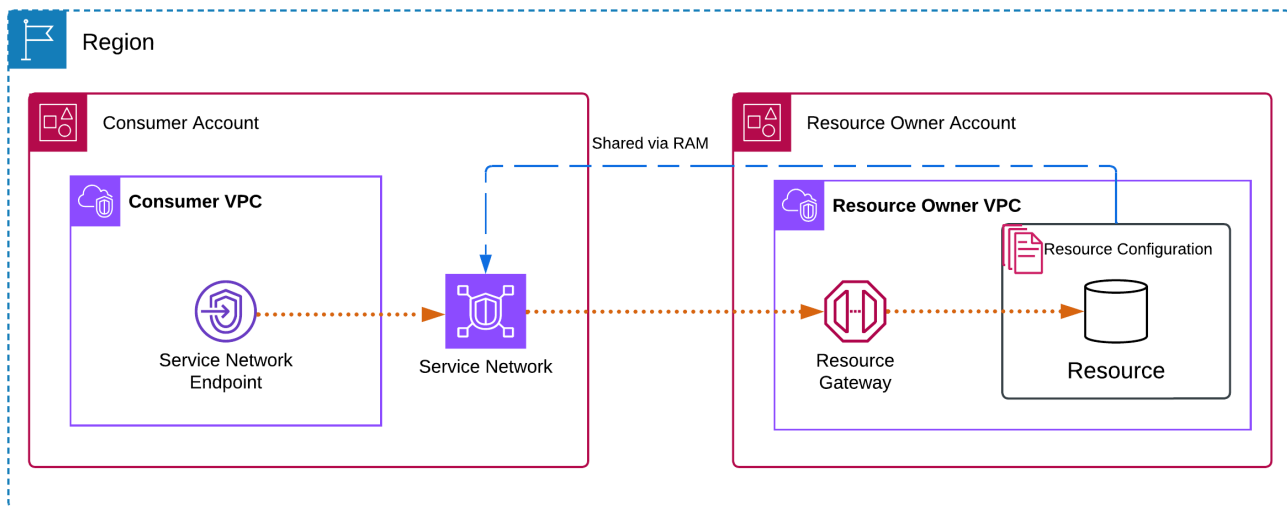
- [Gambaran umum](#)
- [Nama host DNS](#)
- [Resolusi DNS](#)
- [DNS privat](#)

- [Subnet dan Zona Ketersediaan](#)
- [Jenis alamat IP](#)
- [Mengakses jaringan layanan melalui titik akhir jaringan layanan](#)
- [Mengelola titik akhir jaringan layanan](#)

Gambaran umum

Anda dapat membuat jaringan layanan Anda sendiri, atau jaringan layanan dapat dibagikan dengan Anda dari akun lain. Apa pun itu, Anda dapat membuat titik akhir jaringan layanan untuk terhubung ke sana dari VPC Anda. Untuk informasi selengkapnya tentang cara membuat jaringan layanan dan mengaitkan konfigurasi sumber daya dengannya, lihat Panduan <https://docs.aws.amazon.com/vpc-lattice/latest/ug/> Pengguna Amazon VPC Lattice.

Diagram berikut menunjukkan bagaimana titik akhir jaringan layanan di VPC Anda mengakses jaringan layanan.



Koneksi jaringan hanya dapat dimulai dari VPC yang memiliki titik akhir jaringan layanan ke sumber daya dan layanan di jaringan layanan. VPC dengan sumber daya dan layanan tidak dapat memulai koneksi jaringan ke VPC titik akhir.

Nama host DNS

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke jaringan layanan menggunakan titik akhir pribadi. Saat Anda membuat titik akhir VPC jaringan layanan, kami membuat nama DNS Regional

(disebut nama DNS default) untuk setiap sumber daya dan layanan yang dapat Anda gunakan untuk berkomunikasi dengan sumber daya dan layanan dari VPC Anda dan dari lokasi. Alamat IP yang terkait dengan titik akhir dapat berubah. Sebaiknya gunakan DNS alih-alih IP titik akhir untuk menyambung ke jaringan layanan Anda.

Nama DNS default untuk sumber daya di jaringan layanan memiliki sintaks berikut:

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Nama DNS default untuk layanan Lattice di jaringan layanan memiliki sintaks berikut:

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

Jika Anda menggunakan Konsol Manajemen AWS, Anda dapat menemukan nama DNS di bawah tab A sosiasi. Jika Anda menggunakan AWS CLI, gunakan perintah [describe-vpc-endpoint-association](#).

Anda hanya dapat mengaktifkan DNS [pribadi](#) jika jaringan layanan Anda memiliki konfigurasi ARN-type sumber daya ke layanan database Amazon RDS. Dengan DNS pribadi, Anda dapat terus membuat permintaan ke sumber daya menggunakan nama DNS yang disediakan untuk sumber daya oleh AWS layanan, sambil memanfaatkan konektivitas pribadi melalui titik akhir VPC jaringan layanan. Untuk informasi selengkapnya, lihat [the section called “Resolusi DNS”](#).

Resolusi DNS

Saat Anda membuat titik akhir jaringan layanan, kami membuat nama DNS untuk setiap konfigurasi sumber daya dan layanan Lattice yang terkait dengan jaringan layanan. Catatan DNS ini bersifat publik. Oleh karena itu, nama-nama DNS ini dapat diselesaikan secara publik. Namun, permintaan DNS dari luar VPC masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir jaringan layanan. Anda dapat menggunakan nama DNS ini untuk mengakses sumber daya dan layanan dari lokasi, selama Anda memiliki akses ke VPC tempat titik akhir jaringan layanan berada, melalui VPN atau Direct Connect.

DNS privat

Jika Anda mengaktifkan DNS pribadi untuk titik akhir VPC jaringan layanan Anda, dan VPC Anda [mengaktifkan nama host](#) DNS dan resolusi DNS, kami membuat zona host pribadi tersembunyi yang

AWS dikelola untuk konfigurasi sumber daya yang memiliki nama DNS khusus. Zona yang dihosting berisi kumpulan rekaman untuk nama DNS default untuk sumber daya yang menyelesaikannya ke alamat IP pribadi antarmuka jaringan titik akhir layanan di VPC Anda.

Amazon menyediakan server DNS untuk VPC Anda, yang disebut [Route 53 Resolver](#) ver. Route 53 Resolver secara otomatis menyelesaikan nama domain VPC lokal dan rekaman di zona yang dihosting pribadi. Namun, Anda tidak dapat menggunakan Route 53 Resolver dari luar VPC Anda. Jika Anda ingin mengakses titik akhir VPC dari jaringan lokal, Anda dapat menggunakan nama DNS default atau Anda dapat menggunakan titik akhir Route 53 Resolver dan aturan Resolver. Untuk informasi selengkapnya, lihat [Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver](#).

Subnet dan Zona Ketersediaan

Anda dapat mengonfigurasi titik akhir jaringan layanan Anda dengan satu subnet per Zona Ketersediaan. Kami membuat antarmuka jaringan elastis untuk titik akhir VPC di setiap subnet yang Anda tentukan. Kami menetapkan alamat IP ke setiap antarmuka jaringan elastis dari subnetnya sebagai berikut:

- Layanan VPC Lattice (Layer 7) - Kami menetapkan blok /28 (16 alamat IPv4 yang berdekatan) per Zona Ketersediaan untuk semua layanan VPC Lattice yang terkait dengan jaringan layanan. Blok /28 ini dialokasikan ketika titik akhir jaringan layanan dibuat, bahkan jika tidak ada layanan saat ini di jaringan layanan. Blok /28 harus terdiri dari 16 alamat IPv4 yang bersebelahan dan kosong dan tidak dapat tumpang tindih dengan lima alamat cadangan (empat pertama AWS dan IP terakhir). Pastikan ruang alamat bebas yang cukup tersedia. Untuk IPv6, kami juga menetapkan blok /80 per Zona Ketersediaan untuk layanan VPC Lattice.
- Sumber daya VPC Lattice (Layer 4/TCP er) - Kami menetapkan satu alamat IPv4 per konfigurasi sumber daya per Zona Ketersediaan. Ruang alamat yang berdekatan tidak diperlukan untuk sumber daya VPC Lattice. Kami mengalokasikan hingga 63 alamat IP per antarmuka jaringan elastis. Ketika konfigurasi sumber daya tambahan melebihi batas ini, kami membuat antarmuka jaringan elastis lain di subnet yang sama. Untuk IPv6, kami menetapkan blok /80 pada antarmuka jaringan elastis pertama yang dibuat untuk sumber daya; tidak ada antarmuka jaringan elastis tambahan yang dibuat saat menggunakan IPv6. Saat Anda menghapus konfigurasi sumber daya dari jaringan layanan, kami merilis alamat IP terkait. Ketika semua alamat IPv4 pada antarmuka jaringan elastis dilepaskan, kami menghapus antarmuka jaringan elastis.

Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, sebaiknya Anda mengonfigurasi setidaknya dua Zona Ketersediaan untuk setiap titik akhir jaringan layanan dan memastikan bahwa setiap subnet memiliki alamat IPv4 yang cukup tersedia.

Jenis alamat IP

Service-network Endpoint dapat mendukung alamat IPv4, IPv6, atau dual-stack. Endpoint yang mendukung IPv6 dapat menanggapi kueri DNS dengan catatan AAAA. Jenis alamat IP dari titik akhir jaringan layanan harus kompatibel dengan subnet untuk titik akhir sumber daya, seperti yang dijelaskan di sini:

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

Jika titik akhir VPC jaringan layanan mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir VPC jaringan layanan mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan titik akhir tidak dapat dijangkau dari internet. Jika Anda menjelaskan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Mengakses jaringan layanan melalui titik akhir jaringan layanan

Anda dapat mengakses jaringan layanan menggunakan titik akhir jaringan layanan. Titik akhir jaringan layanan menyediakan akses pribadi ke konfigurasi sumber daya dan layanan dalam jaringan layanan.

Prasyarat

Untuk membuat titik akhir jaringan layanan, Anda harus memenuhi prasyarat berikut.

- Anda harus memiliki jaringan layanan yang dibuat oleh Anda atau dibagikan dengan Anda dari akun lain melalui AWS RAM.

- Jika jaringan layanan dibagikan dengan Anda dari akun lain, Anda harus meninjau dan menerima pembagian sumber daya yang berisi jaringan layanan. Untuk informasi selengkapnya, [lihat Menerima dan menolak undangan](#) di Panduan AWS RAM Pengguna.
- Untuk layanan VPC Lattice yang terkait dengan jaringan layanan, titik akhir jaringan layanan memerlukan blok /28 yang berdekatan (16 alamat IPv4) per Zona Ketersediaan. Blok /28 ini dialokasikan saat titik akhir dibuat, bahkan jika tidak ada layanan saat ini di jaringan layanan. Blok /28 harus terdiri dari 16 alamat IPv4 yang bersebelahan dan kosong dan tidak dapat tumpang tindih dengan lima alamat cadangan (empat pertama dan AWS IP terakhir di subnet). Untuk IPv6, blok /80 per Zona Ketersediaan dialokasikan untuk layanan VPC Lattice. Pastikan ruang alamat bebas yang cukup tersedia di setiap subnet yang Anda pilih.
- Untuk sumber daya VPC Lattice (Layer 4/TCP) yang terkait dengan jaringan layanan, diperlukan satu alamat IPv4 per konfigurasi sumber daya per Zona Ketersediaan. Ruang alamat yang berdekatan tidak diperlukan. Hingga 63 alamat IP dapat dialokasikan per antarmuka jaringan elastis. Ketika konfigurasi sumber daya tambahan melebihi batas ini, antarmuka jaringan elastis tambahan dibuat di subnet yang sama. Untuk IPv6, blok /80 ditetapkan pada antarmuka jaringan elastis pertama yang dibuat untuk sumber daya; tidak ada antarmuka jaringan elastis tambahan yang dibuat saat menggunakan IPv6.

Jika Anda perlu menghindari penggunaan alamat IP VPC CIDR, atau mengantisipasi sejumlah besar konfigurasi sumber daya yang terkait dengan jaringan layanan, pertimbangkan untuk menggunakan asosiasi VPC jaringan layanan sebagai gantinya. Untuk informasi selengkapnya, lihat [M mengelola asosiasi titik akhir VPC](#) di Panduan Pengguna Amazon VPC Lattice.

Membuat titik akhir jaringan layanan

Buat titik akhir jaringan layanan untuk mengakses jaringan layanan yang dibagikan dengan Anda. Setelah Anda membuat titik akhir jaringan layanan, Anda hanya dapat mengubah grup atau tag keamanannya.

Untuk membuat titik akhir jaringan layanan

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih T itik Akhir.
3. Pilih Buat titik akhir.
4. Anda dapat menentukan nama untuk membuatnya lebih mudah untuk menemukan dan mengelola titik akhir.

5. Untuk Jenis, pilih Jaringan layanan.
6. Untuk Jaringan layanan, pilih jaringan layanan.
7. Untuk Pengaturan jaringan, pilih VPC tempat Anda akan mengakses jaringan layanan.
8. Jika, Anda ingin mengonfigurasi dukungan DNS pribadi, pilih Pengaturan tambahan, Aktifkan nama DNS pribadi. Untuk menggunakan fitur ini, pastikan atribut Aktifkan nama host DNS dan Aktifkan dukungan DNS diaktifkan untuk VPC Anda.
9. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir.

Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, sebaiknya konfigurasi setidaknya dua Zona Ketersediaan untuk setiap titik akhir VPC.

10. Untuk Grup keamanan, pilih grup keamanan.

Jika Anda tidak menentukan grup keamanan, kami mengaitkan grup keamanan default untuk VPC.

11. Pilih Buat titik akhir.

Untuk membuat titik akhir jaringan layanan menggunakan baris perintah

- [buat-titik akhir vpc \(\)](#) AWS CLI
- [New-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Mengelola titik akhir jaringan layanan

Setelah Anda membuat titik akhir jaringan layanan, Anda dapat memperbarui grup atau tag keamanannya.

Tugas

- [Hapus titik akhir](#)
- [Memperbarui titik akhir jaringan layanan](#)

Hapus titik akhir

Ketika Anda selesai dengan titik akhir VPC, Anda dapat menghapusnya.

Untuk menghapus titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir jaringan layanan.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir menggunakan baris perintah

- [hapus titik akhir vpc \(\)](#) AWS CLI
- [Remove-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Memperbarui titik akhir jaringan layanan

Anda dapat memperbarui titik akhir VPC.

Untuk memperbarui titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, dan opsi yang sesuai.
5. Ikuti langkah-langkah konsol untuk mengirimkan pembaruan.

Untuk memperbarui titik akhir menggunakan baris perintah

- [modify-vpc-endpoint \(\)](#) AWS CLI
- [Edit-EC2VpcEndpoint](#)(Alat untuk Windows PowerShell)

Konfigurasi sumber daya untuk sumber daya VPC

Konfigurasi sumber daya mewakili sumber daya individu, sekelompok sumber daya, atau daftar rentang CIDR yang ingin Anda buat dapat diakses oleh klien di VPC dan akun lain. Dengan menentukan konfigurasi sumber daya, Anda dapat mengizinkan konektivitas jaringan pribadi, aman, searah ke sumber daya di VPC Anda dari klien di VPC dan akun lain. Konfigurasi sumber daya dikaitkan dengan gateway sumber daya yang melaluinya menerima lalu lintas.

Daftar Isi

- [Jenis konfigurasi sumber daya](#)
- [Gateway sumber daya](#)
- [Nama domain khusus untuk penyedia sumber daya](#)
- [Nama domain khusus untuk konsumen sumber daya](#)
- [Nama domain khusus untuk pemilik jaringan layanan](#)
- [Definisi sumber daya](#)
- [Protokol](#)
- [Rentang pelabuhan](#)
- [Mengakses sumber daya](#)
- [Asosiasi dengan jenis jaringan layanan](#)
- [Jenis jaringan layanan](#)
- [Berbagi konfigurasi sumber daya melalui AWS RAM](#)
- [Memantau](#)
- [Membuat konfigurasi sumber daya di VPC Lattice](#)
- [Mengelola pengaitan konfigurasi sumber daya VPC Lattice](#)

Jenis konfigurasi sumber daya

Konfigurasi sumber daya dapat terdiri dari beberapa jenis. Jenis yang berbeda membantu mewakili berbagai jenis sumber daya. Jenis-jenisnya adalah:

- Konfigurasi sumber daya tunggal: Alamat IP atau nama domain. Itu dapat dibagikan secara independen.

- Konfigurasi sumber daya grup: Kumpulan konfigurasi sumber daya anak. Itu dapat dibagikan secara independen.
- Konfigurasi sumber daya anak: Anggota konfigurasi sumber daya Grup. Ini mewakili alamat IP atau nama domain. Itu tidak dapat dibagikan secara independen, dan hanya dapat dibagikan sebagai bagian dari grup. Itu dapat ditambahkan dan dihapus dari grup dengan mulus. Ketika ditambahkan, secara otomatis dapat diakses oleh mereka yang dapat mengakses grup.
- Konfigurasi sumber daya ARN: Jenis sumber daya yang didukung yang disediakan oleh AWS layanan. Misalnya, database Amazon RDS. Konfigurasi sumber daya anak dikelola secara otomatis oleh AWS. Itu dapat dibagikan secara independen.
- Konfigurasi sumber daya CIDR: Daftar rentang CIDR. Itu dapat dibagikan secara independen.

Gateway sumber daya

Konfigurasi sumber daya dikaitkan dengan gateway sumber daya. Gateway sumber daya adalah sekumpulan ENI yang berfungsi sebagai titik masuk ke VPC tempat sumber daya berada. Beberapa konfigurasi sumber daya dapat dikaitkan dengan gateway sumber daya yang sama. Ketika klien di VPC atau akun lain mengakses sumber daya di VPC Anda, sumber daya melihat lalu lintas yang datang secara lokal dari gateway sumber daya di VPC tersebut.

Nama domain khusus untuk penyedia sumber daya

Penyedia sumber daya dapat melampirkan nama domain khusus ke konfigurasi sumber daya, seperti `example.com`, yang dapat digunakan konsumen sumber daya untuk mengakses konfigurasi sumber daya. Nama domain khusus dapat dimiliki dan diverifikasi oleh penyedia sumber daya, atau dapat berupa pihak ketiga atau AWS domain. Penyedia sumber daya dapat menggunakan konfigurasi sumber daya untuk berbagi cluster cache dan klaster Kafka, TLS-based aplikasi, atau AWS sumber daya lainnya.

Pertimbangan berikut berlaku untuk penyedia konfigurasi sumber daya:

- Konfigurasi sumber daya hanya dapat memiliki satu domain khusus.
- Nama domain kustom dari konfigurasi sumber daya tidak dapat diubah.
- Nama domain kustom terlihat oleh semua konsumen konfigurasi sumber daya.
- Anda dapat memverifikasi nama domain kustom Anda menggunakan proses verifikasi nama domain di VPC Lattice. Untuk informasi selengkapnya, lihat <https://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html>.

- Untuk konfigurasi sumber daya tipe grup dan anak, Anda harus terlebih dahulu menentukan domain grup pada konfigurasi sumber daya grup. Setelah itu, konfigurasi sumber daya anak dapat memiliki domain kustom yang merupakan subdomain dari domain grup. Jika grup tidak memiliki domain grup, Anda dapat menggunakan nama domain kustom apa pun untuk anak, tetapi VPC Lattice tidak akan menyediakan zona yang dihosting untuk nama domain anak di VPC konsumen sumber daya.
- Nama domain khusus tidak didukung untuk konfigurasi sumber daya CIDR.

Nama domain khusus untuk konsumen sumber daya

Ketika konsumen sumber daya mengaktifkan konektivitas ke konfigurasi sumber daya yang memiliki nama domain khusus, mereka dapat mengizinkan VPC Lattice mengelola zona host pribadi Route 53 di VPC mereka. Konsumen sumber daya memiliki opsi terperinci untuk domain mana yang ingin mereka izinkan VPC Lattice mengelola zona pribadi yang dihosting.

Konsumen sumber daya dapat mengatur `private-dns-enabled` parameter saat mengaktifkan konektivitas ke konfigurasi sumber daya melalui titik akhir sumber daya, titik akhir jaringan layanan, atau asosiasi VPC jaringan layanan. Seiring dengan `private-dns-enabled` parameter, konsumen dapat menggunakan opsi DNS untuk menentukan domain mana yang mereka inginkan untuk VPC Lattice mengelola zona pribadi yang dihosting. Konsumen dapat memilih antara preferensi DNS pribadi berikut:

ALL_DOMAINS

VPC Lattice menyediakan zona host pribadi untuk semua nama domain khusus.

VERIFIED_DOMAINS_ONLY

VPC Lattice menyediakan zona pribadi yang dihosting hanya jika nama domain khusus telah diverifikasi oleh penyedia.

VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS

VPC Lattice menyediakan zona host pribadi untuk semua nama domain kustom terverifikasi dan nama domain lain yang ditentukan oleh konsumen sumber daya. Konsumen sumber daya menentukan nama domain dalam `private DNS specified domains` parameter.

SPECIFIED_DOMAINS_ONLY

VPC Lattice menyediakan zona host pribadi untuk nama domain yang ditentukan oleh konsumen sumber daya. Konsumen sumber daya menentukan nama domain dalam `private DNS specified domains` parameter.

Saat Anda mengaktifkan DNS pribadi, VPC Lattice membuat zona pribadi yang dihosting di VPC Anda untuk nama domain kustom yang terkait dengan konfigurasi sumber daya. Secara default, preferensi DNS pribadi diatur ke `VERIFIED_DOMAINS_ONLY`. Ini berarti bahwa zona pribadi yang dihosting dibuat hanya jika nama domain kustom telah diverifikasi oleh penyedia sumber daya. Jika Anda menyetel preferensi DNS pribadi ke `ALL_DOMAINS` atau `SPECIFIED_DOMAINS_ONLY` kemudian VPC Lattice membuat zona yang dihosting pribadi terlepas dari status verifikasi nama domain kustom. Ketika zona pribadi yang dihosting dibuat untuk domain tertentu, semua lalu lintas ke domain tersebut dari VPC Anda dialihkan melalui VPC Lattice. Kami menyarankan Anda menggunakan `ALL_DOMAINS`, `VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`, atau `SPECIFIED_DOMAINS_ONLY` preferensi hanya jika Anda ingin lalu lintas ke nama domain khusus ini melewati VPC Lattice.

Sebaiknya konsumen sumber daya menyetel preferensi DNS pribadi mereka ke `VERIFIED_DOMAINS_ONLY`. Hal ini memungkinkan konsumen memperketat perimeter keamanan mereka dengan hanya mengizinkan VPC Lattice menyediakan zona yang dihosting pribadi untuk domain terverifikasi di akun konsumen sumber daya.

Untuk memilih domain di domain tertentu DNS pribadi, konsumen sumber daya dapat memasukkan nama domain yang memenuhi syarat penuh, seperti `my.example.com` atau menggunakan wildcard seperti `*.example.com`.

Pertimbangan berikut berlaku untuk konsumen konfigurasi sumber daya:

- Parameter yang diaktifkan DNS pribadi tidak dapat diubah.
- DNS pribadi harus diaktifkan pada asosiasi sumber daya jaringan layanan untuk zona host pribadi yang akan dibuat di VPC. Untuk konfigurasi sumber daya, status diaktifkan DNS pribadi dari asosiasi sumber daya jaringan layanan menggantikan status aktif DNS pribadi dari titik akhir jaringan layanan atau asosiasi VPC jaringan layanan.

Untuk konfigurasi sumber daya yang merupakan target nama domain, entri zona yang dihosting pribadi tidak dibuat jika berikut ini benar:

- Gateway sumber daya berada di VPC yang sama dengan asosiasi VPC jaringan layanan VPC endpoint/service jaringan VPC.
- Resolusi DNS diatur ke IN_VPC pada gateway sumber daya.
- Nama domain kustom atau domain grup adalah domain tingkat yang sama atau lebih tinggi dari target nama domain.

Untuk konfigurasi sumber daya yang bertipe ARN, VPC Lattice tidak membuat entri zona yang dihosting pribadi jika berikut ini benar:

- Gateway sumber daya berada di VPC yang sama dengan asosiasi VPC jaringan layanan VPC endpoint/service jaringan VPC.

Nama domain khusus untuk pemilik jaringan layanan

Properti yang diaktifkan DNS pribadi dari asosiasi sumber daya jaringan layanan menggantikan properti yang diaktifkan DNS pribadi dari titik akhir jaringan layanan dan asosiasi VPC jaringan layanan.

Jika pemilik jaringan layanan membuat asosiasi sumber daya jaringan layanan dan tidak mengaktifkan DNS pribadi, VPC Lattice tidak akan menyediakan zona host pribadi untuk konfigurasi sumber daya tersebut di VPC mana pun yang terhubung ke jaringan layanan, meskipun DNS pribadi diaktifkan pada titik akhir jaringan layanan atau asosiasi VPC jaringan layanan.

Untuk konfigurasi sumber daya tipe ARN, bendera DNS pribadi adalah benar dan tidak dapat diubah. Oleh karena itu, VPC Lattice menyediakan zona host pribadi untuk jenis sumber daya ARN terlepas dari pengaturan properti DNS pribadi dari titik akhir jaringan layanan dan asosiasi VPC jaringan layanan, kecuali ketika gateway sumber daya juga berada di VPC yang sama. Dengan kata lain, ketika VPC adalah konsumen dan penyedia untuk konfigurasi sumber daya jenis ARN, VPC Lattice melewatkan pembuatan zona yang dihosting pribadi di VPC tersebut.

Definisi sumber daya

Dalam konfigurasi sumber daya, identifikasi sumber daya dengan salah satu cara berikut:

- Dengan Nama Sumber Daya Amazon (ARN): Jenis sumber daya yang didukung yang disediakan oleh AWS layanan dapat diidentifikasi oleh ARN mereka. Hanya database Amazon RDS yang

didukung. Anda tidak dapat membuat konfigurasi sumber daya untuk cluster yang dapat diakses publik.

- Dengan target nama domain: Anda dapat menggunakan nama domain apa pun. Jika Anda menggunakan server DNS pribadi atau domain Anda berada di zona host pribadi Route 53, maka gateway sumber daya harus memiliki resolusi DNS yang disetel ke IN_VPC. Jika nama domain Anda menunjuk ke IP yang berada di luar VPC Anda, Anda harus memiliki gateway NAT di VPC Anda. Domain-name target yang diselesaikan ke alamat IPv6 publik tidak didukung.
- Dengan alamat IP: Untuk IPv4, tentukan IP pribadi dari rentang berikut: 10.0.0. 0/8, 100,64,0. 0/10, 172.16.0. 0/12, 192,168,0. 0/16. Untuk IPv6, tentukan IP dari VPC. IP publik tidak didukung.
- Dengan rentang CIDR: Untuk konfigurasi sumber daya tipe CIDR, tentukan daftar CIDR yang ingin Anda bagikan (misalnya, 10.0.0. 0/24). CIDR harus dapat dijangkau dari gateway sumber daya. Untuk menyediakan akses jaringan penuh, tentukan 0.0.0. 0/0 jika menggunakan IPv4 atau ::/0 jika menggunakan IPv6.

Protokol

Ketika Anda membuat konfigurasi sumber daya, Anda dapat menentukan protokol yang akan didukung sumber daya. Saat ini, hanya protokol TCP yang didukung.

Untuk konfigurasi sumber daya CIDR, protokol harus TCP_UDP: hanya TCP yang didukung untuk lalu lintas aplikasi, UDP hanya didukung untuk kueri DNS.

Rentang pelabuhan

Saat Anda membuat konfigurasi sumber daya, Anda dapat menentukan port yang akan menerima permintaan. Akses klien di port lain tidak akan diizinkan.

Mengakses sumber daya

Konsumen dapat mengakses konfigurasi sumber daya langsung dari VPC mereka menggunakan titik akhir VPC atau melalui jaringan layanan. Sebagai konsumen, Anda dapat mengaktifkan akses dari VPC ke konfigurasi sumber daya yang ada di akun Anda atau yang telah dibagikan dengan Anda dari akun lain melalui AWS RAM.

- Mengakses konfigurasi sumber daya secara langsung

Anda dapat mengakses konfigurasi sumber daya secara langsung melalui titik akhir sumber daya AWS PrivateLink berbasis dan titik akhir terowongan. Anda dapat membuat titik akhir sumber daya di VPC untuk mengakses konfigurasi sumber daya tipe ARN, Single, dan Group, dan dapat membuat titik akhir terowongan untuk mengakses konfigurasi sumber daya tipe CIDR. Untuk informasi selengkapnya tentang cara membuat titik akhir sumber daya dan terowongan, lihat Meng [akses sumber daya VPC](#) dan Meng [akses segmen jaringan](#) di panduan AWS PrivateLink pengguna.

- Mengakses konfigurasi sumber daya melalui jaringan layanan

Anda dapat mengaitkan konfigurasi sumber daya dengan jaringan layanan, dan menghubungkan VPC Anda ke jaringan layanan. Anda dapat menghubungkan VPC Anda ke jaringan layanan baik melalui asosiasi atau menggunakan titik akhir jaringan layanan AWS PrivateLink berbasis. Konfigurasi sumber daya CIDR tidak dapat dikaitkan dengan jaringan layanan.

Untuk informasi selengkapnya tentang asosiasi jaringan layanan, lihat Mengel [ola asosiasi untuk jaringan](#) layanan VPC Lattice.

Untuk informasi selengkapnya tentang titik akhir VPC jaringan layanan, lihat [Akses jaringan layanan](#) di panduan AWS PrivateLink pengguna.

Saat DNS pribadi diaktifkan untuk VPC Anda, Anda tidak dapat membuat titik akhir sumber daya dan titik akhir jaringan layanan untuk konfigurasi sumber daya yang sama.

Asosiasi dengan jenis jaringan layanan

Ketika Anda berbagi konfigurasi sumber daya dengan akun konsumen, misalnya, melalui Account-B AWS RAM, Account-B dapat mengakses konfigurasi sumber daya baik secara langsung melalui titik akhir sumber daya atau titik akhir terowongan, atau melalui jaringan layanan. Konfigurasi sumber daya CIDR tidak dapat diakses melalui jaringan layanan. Mereka hanya dapat diakses langsung melalui titik akhir terowongan.

Untuk mengakses konfigurasi sumber daya melalui jaringan layanan, Account-B harus mengaitkan konfigurasi sumber daya dengan jaringan layanan. Jaringan layanan dapat dibagikan antar akun. Jadi, Account-B dapat berbagi jaringan layanan mereka (yang terkait dengan konfigurasi sumber daya) Account-C, membuat sumber daya Anda dapat diakses dari Account-C.

Untuk mencegah berbagi transitif seperti itu, Anda dapat menentukan bahwa konfigurasi sumber daya Anda tidak dapat ditambahkan ke jaringan layanan yang dapat dibagikan antar akun. Jika Anda menentukan ini, maka Account-B tidak akan dapat menambahkan konfigurasi sumber daya Anda ke jaringan layanan yang dibagikan atau dapat dibagikan dengan akun lain di masa mendatang.

Jenis jaringan layanan

Ketika Anda berbagi konfigurasi sumber daya dengan akun lain, misalnya melalui Account-B AWS RAM, Account-B dapat mengakses sumber daya dengan salah satu dari empat cara:

- Menggunakan titik akhir sumber daya AWS PrivateLink berbasis (untuk konfigurasi sumber daya Tunggal, Grup, dan ARN).
- Menggunakan titik akhir terowongan AWS PrivateLink berbasis (untuk konfigurasi sumber daya CIDR).
- Menggunakan titik akhir jaringan layanan AWS PrivateLink berbasis.
- Menggunakan asosiasi VPC jaringan layanan.

Saat Anda menggunakan asosiasi jaringan layanan, setiap sumber daya diberi IP per subnet dari 129.224.0. 0/17 blok, yang AWS dimiliki dan tidak dapat dirutekan. Ini merupakan tambahan dari daftar awalan ter [kelola](#) yang digunakan VPC Lattice untuk merutekan lalu lintas ke layanan melalui jaringan VPC Lattice. Kedua IP ini diperbarui ke tabel rute VPC Anda.

Untuk titik akhir jaringan layanan dan asosiasi VPC jaringan layanan, konfigurasi sumber daya harus dimasukkan ke dalam Account-B jaringan layanan. Jaringan layanan dapat dibagikan antar akun. Jadi, Account-B dapat berbagi jaringan layanan mereka (yang berisi konfigurasi sumber daya) dengan Account-C, membuat sumber daya Anda dapat diakses dari Account-C. Untuk mencegah berbagi transitif seperti itu, Anda dapat melarang konfigurasi sumber daya ditambahkan ke jaringan layanan yang dapat dibagikan antar akun. Jika Anda tidak mengizinkan ini Account-B, maka tidak akan dapat menambahkan konfigurasi sumber daya Anda ke jaringan layanan yang dibagikan atau dapat dibagikan dengan akun lain.

Berbagi konfigurasi sumber daya melalui AWS RAM

Konfigurasi sumber daya terintegrasi dengan AWS Resource Access Manager. Anda dapat membagikan konfigurasi sumber daya Anda dengan akun lain melalui AWS RAM. Saat Anda berbagi konfigurasi sumber daya dengan AWS akun, klien di akun tersebut dapat mengakses sumber daya

secara pribadi. Anda dapat berbagi konfigurasi sumber daya menggunakan berbagi [sumber daya](#) di AWS RAM.

Gunakan AWS RAM konsol, untuk melihat berbagi sumber daya yang telah ditambahkan, sumber daya bersama yang dapat Anda akses, dan AWS akun yang telah berbagi sumber daya dengan Anda. Untuk informasi selengkapnya, lihat [Sumber daya yang dibagikan dengan Anda](#) di Panduan AWS RAM Pengguna.

Untuk mengakses sumber daya dari VPC lain di akun yang sama dengan konfigurasi sumber daya, Anda tidak perlu membagikan konfigurasi sumber daya melalui AWS RAM.

Memantau

Anda dapat mengaktifkan log pemantauan pada konfigurasi sumber daya Anda. Anda dapat memilih tujuan untuk mengirim log.

Membuat konfigurasi sumber daya di VPC Lattice

Buat konfigurasi sumber daya.

Konsol Manajemen AWS

Untuk membuat konfigurasi sumber daya menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih Buat konfigurasi sumber daya.
4. Masukkan nama yang unik dalam AWS akun Anda. Anda tidak dapat mengubah nama ini setelah konfigurasi sumber daya dibuat.
5. Untuk Jenis konfigurasi, pilih Sumber daya untuk sumber daya tunggal atau anak atau grup Sumber daya untuk grup sumber daya anak.
6. Pilih gateway sumber daya yang sebelumnya Anda buat atau buat sekarang.
7. (Opsional) Untuk memasukkan nama domain khusus, lakukan salah satu hal berikut:
 - Jika Anda memiliki konfigurasi sumber daya tipe tunggal, Anda dapat memasukkan nama domain khusus. Konsumen sumber daya dapat menggunakan nama domain ini untuk mengakses konfigurasi sumber daya Anda.

- Jika Anda memiliki konfigurasi sumber daya tipe grup dan anak, Anda harus terlebih dahulu menentukan domain grup pada konfigurasi sumber daya grup. Selanjutnya, konfigurasi sumber daya anak dapat memiliki domain kustom yang merupakan subdomain dari domain grup.

8. (Opsional) Masukkan ID verifikasi.

Berikan ID verifikasi jika Anda ingin nama domain Anda diverifikasi. Ini memungkinkan konsumen sumber daya tahu bahwa Anda memiliki nama domain.

9. Pilih pengidentifikasi untuk sumber daya yang Anda ingin diwakili oleh konfigurasi sumber daya ini.
10. Pilih rentang port tempat Anda ingin berbagi sumber daya.
11. Untuk pengaturan Asosiasi, tentukan apakah konfigurasi sumber daya ini dapat dikaitkan dengan jaringan layanan yang dapat dibagikan.
12. Untuk Bagikan konfigurasi sumber daya, pilih pembagian sumber daya yang mengidentifikasi prinsipal yang dapat mengakses sumber daya ini.
13. (Opsional) Untuk Pemantauan, aktifkan log akses Sumber daya dan tujuan pengiriman jika Anda ingin memantau permintaan dan tanggapan ke dan dari konfigurasi sumber daya.
14. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
15. Pilih Buat konfigurasi sumber daya.

AWS CLI

Perintah [create-resource-configuration](#) berikut membuat konfigurasi sumber daya tunggal dan menghubungkannya dengan nama domain kustom. `example.com`

```
aws vpc-lattice create-resource-configuration \
  --name my-resource-config \
  --type SINGLE \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
  --custom-domain-name example.com \
  --verification-id dv-aaaa0000000111111
```

Perintah [create-resource-configuration](#) berikut membuat konfigurasi sumber daya grup dan mengaitkannya dengan nama domain kustom. `example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --domain-verification-identifier dv-aaaa00000000111111
```

Perintah [create-resource-configuration](#) berikut membuat konfigurasi sumber daya anak dan menghubungkannya dengan nama domain kustom. `child.example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-child \
  --type CHILD \
  --resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-west-2.elb.amazonaws.com,ipAddressType=IPV4}' \
  --resource-configuration-group-identifier rcfg-07129f3acded87626 \
  --custom-domain-name child.example.com
```

Mengelola pengaitan konfigurasi sumber daya VPC Lattice

Akun konsumen tempat Anda berbagi konfigurasi sumber daya, dan klien di akun Anda, dapat mengakses konfigurasi sumber daya baik secara langsung menggunakan titik akhir VPC sumber daya atau melalui titik akhir jaringan layanan. Akibatnya, konfigurasi sumber daya Anda akan memiliki asosiasi titik akhir dan asosiasi jaringan layanan.

Kelola asosiasi sumber daya jaringan layanan

Buat atau hapus asosiasi jaringan layanan.

Note

Jika Anda menerima pesan yang ditolak akses saat membuat hubungan antara konfigurasi jaringan layanan dan sumber daya, periksa versi AWS RAM kebijakan Anda dan pastikan itu adalah versi 2. Untuk informasi selengkapnya, lihat panduan [AWS RAM pengguna](#).

Untuk mengelola asosiasi layanan-jaringan menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.

2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih nama konfigurasi sumber daya untuk membuka halaman detailnya.
4. Pilih tab asosiasi jaringan layanan.
5. Pilih Buat asosiasi.
6. Pilih jaringan layanan dari jaringan layanan VPC Lattice. Untuk membuat jaringan layanan, pilih Buat jaringan VPC Lattice.
7. (Opsional) Untuk menambahkan tag, perluas Tag asosiasi layanan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
8. (Opsional) Untuk mengaktifkan nama DNS pribadi untuk asosiasi sumber daya jaringan layanan ini pilih aktifkan nama DNS pribadi. Untuk informasi selengkapnya, lihat [the section called “Nama domain khusus untuk pemilik jaringan layanan”](#).
9. Pilih Simpan perubahan.
10. Untuk menghapus asosiasi, pilih kotak centang untuk asosiasi dan kemudian pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **confirm**, lalu pilih Hapus.

Untuk membuat asosiasi jaringan layanan menggunakan AWS CLI

Gunakan perintah [create-service-network-resource-association](#).

Untuk menghapus asosiasi jaringan layanan menggunakan AWS CLI

Gunakan perintah [delete-service-network-resource-association](#).

Kelola asosiasi titik akhir VPC sumber daya

Akun konsumen dengan akses ke konfigurasi sumber daya atau klien di akun Anda dapat mengakses konfigurasi sumber daya menggunakan titik akhir VPC sumber daya. Jika konfigurasi sumber daya Anda memiliki nama domain khusus, Anda dapat menggunakan mengaktifkan DNS pribadi untuk mengizinkan VPC Lattice menyediakan zona pribadi yang dihosting untuk titik akhir sumber daya atau titik akhir jaringan layanan Anda. Dengan ini, klien dapat langsung menggulung nama domain untuk mengakses konfigurasi sumber daya. Untuk informasi selengkapnya, lihat [the section called “Nama domain khusus untuk konsumen sumber daya”](#).

Konsol Manajemen AWS

1. Untuk membuat asosiasi titik akhir baru, buka PrivateLink dan Lattice di panel navigasi kiri dan pilih Endpoints.

2. Pilih Buat titik akhir.
3. Pilih konfigurasi sumber daya yang ingin Anda sambungkan ke VPC Anda.
4. Pilih VPC, subnet, dan grup keamanan.
5. (Opsional) Untuk mengaktifkan DNS pribadi dan mengonfigurasi opsi DNS, pilih Aktifkan nama DNS.
6. (Opsional) Untuk menandai titik akhir VPC Anda, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
7. Pilih Buat titik akhir.

AWS CLI

Perintah [create-vpc-endpoint](#) berikut membuat titik akhir VPC yang menggunakan DNS pribadi. Preferensi DNS pribadi diatur ke VERIFIED_AND_SELECTED dan domain yang dipilih adalah `example.com` dan `example.org`. VPC Lattice hanya menyediakan zona yang dihosting pribadi untuk domain terverifikasi atau `example.com` atau `example.org`.

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Resource \
  --vpc-id vpc-111122223333aabbcc \
  --subnet-ids subnet-0011aabbcc2233445 \
  --resource-configuration-arn arn:aws:vpc-lattice:us-
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \
  --private-dns-enabled \
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \
  --private-domains-set example.com, example.org
```

Untuk membuat asosiasi titik akhir VPC menggunakan AWS CLI

Gunakan perintah [create-vpc-endpoint](#).

Untuk menghapus asosiasi titik akhir VPC menggunakan AWS CLI

Gunakan perintah [delete-vpc-endpoint](#).

Gerbang sumber daya di VPC Lattice

Gateway sumber daya adalah titik lalu lintas masuk ke VPC tempat sumber daya berada. Ini mencakup beberapa Zona Ketersediaan.

VPC harus memiliki gateway sumber daya jika Anda berencana membuat sumber daya di dalam VPC dapat diakses dari VPC atau akun lain. Setiap sumber daya yang Anda bagikan dikaitkan dengan gateway sumber daya. Ketika klien di VPC atau akun lain mengakses sumber daya di VPC Anda, sumber daya melihat lalu lintas yang datang secara lokal dari gateway sumber daya di VPC tersebut. IP sumber lalu lintas adalah alamat IP gateway sumber daya. Anda dapat menetapkan beberapa alamat IP ke gateway sumber daya untuk memungkinkan lebih banyak koneksi jaringan dengan sumber daya. Beberapa sumber daya dalam VPC dapat dikaitkan dengan gateway sumber daya yang sama.

Gateway sumber daya tidak menyediakan kemampuan penyeimbangan beban.

Daftar Isi

- [Pertimbangan-pertimbangan](#)
- [Grup keamanan](#)
- [Jenis alamat IP](#)
- [Alamat IPv4 per ENI](#)
- [Resolusi DNS Konfigurasi Sumber Daya](#)
- [Membuat gateway sumber daya di VPC Lattice](#)
- [Menghapus gateway sumber daya di VPC Lattice](#)

Pertimbangan-pertimbangan

Pertimbangan berikut berlaku untuk gateway sumber daya:

- Agar sumber daya dapat diakses dari semua Zona [Ketersediaan](#), Anda harus membuat gateway sumber daya untuk menjangkau sebanyak mungkin Zona Ketersediaan.
- Setidaknya satu Zona Ketersediaan dari titik akhir VPC dan gateway sumber daya harus tumpang tindih.
- VPC dapat memiliki maksimum 100 gateway sumber daya. Untuk informasi selengkapnya, lihat [Kuda untuk Lattice VPC](#).

- Anda tidak dapat membuat gateway sumber daya di subnet bersama.

Grup keamanan

Anda dapat melampirkan grup keamanan ke gateway sumber daya. Aturan grup keamanan untuk gateway sumber daya mengontrol lalu lintas keluar dari gateway sumber daya ke sumber daya.

Aturan keluar yang disarankan untuk lalu lintas yang mengalir dari gateway sumber daya ke sumber daya database

Agar lalu lintas mengalir dari gateway sumber daya ke sumber daya, Anda harus membuat aturan keluar untuk protokol pendengar dan rentang port yang diterima sumber daya.

Tujuan	Protokol	Rentang port	Komentar
<i>CIDR range for resource</i>	TCP	3306	Memungkinkan lalu lintas dari gateway sumber daya ke database.

Jenis alamat IP

Gateway sumber daya dapat memiliki alamat IPv4, IPv6, atau dual-stack. Jenis alamat IP gateway sumber daya harus kompatibel dengan subnet gateway sumber daya dan jenis alamat IP sumber daya, seperti yang dijelaskan di sini:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan gateway Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4, dan sumber daya juga memiliki alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan gateway Anda. Opsi ini didukung hanya jika semua subnet yang dipilih adalah IPv6-only subnet, dan sumber daya juga memiliki alamat IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan gateway Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6, dan sumber daya memiliki alamat IPv4 atau IPv6.

Jenis alamat IP gateway sumber daya tidak tergantung pada jenis alamat IP klien atau titik akhir VPC yang melaluinya sumber daya diakses.

Alamat IPv4 per ENI

Jika gateway sumber daya Anda memiliki tipe alamat IP IPv4 atau dual-stack, Anda dapat mengonfigurasi jumlah alamat IPv4 yang ditetapkan untuk setiap ENI gateway sumber daya Anda. Saat Anda membuat gateway sumber daya, Anda memilih dari 1 hingga 62 alamat IPv4. Setelah Anda mengatur jumlah alamat IPv4, nilainya tidak dapat diubah.

Alamat IPv4 digunakan untuk terjemahan alamat jaringan dan menentukan jumlah maksimum koneksi IPv4 bersamaan ke sumber daya. Secara default, semua gateway sumber daya ditetapkan 16 alamat IPv4 per ENI. Ini adalah jumlah IP yang cocok untuk membentuk koneksi dengan sumber daya backend Anda.

Jika gateway sumber daya Anda menggunakan jenis alamat IPv6, gateway sumber daya secara otomatis menerima /80 CIDR per ENI. Nilai ini tidak dapat diubah.

Resolusi DNS Konfigurasi Sumber Daya

Anda dapat menentukan bagaimana gateway sumber daya melakukan resolusi DNS untuk konfigurasi sumber daya yang merupakan target nama domain. Properti ini tetap. Anda dapat memilih:

- **PUBLIK (default)** - Nama domain diselesaikan menggunakan resolver DNS publik.
- **IN_VPC** - Nama domain diselesaikan menggunakan server DNS yang dikonfigurasi dalam set opsi DHCP dari VPC tempat gateway sumber daya berada. Anda harus menggunakan ini jika Anda menggunakan server DNS pribadi atau target nama domain Anda berada di zona host pribadi Route 53.

Jika resolusi DNS adalah **IN_VPC**, Anda tidak dapat melampirkan konfigurasi sumber daya yang ditentukan oleh ARN ke gateway sumber daya. Anda tidak dapat mengatur resolusi DNS ke **IN_VPC** jika gateway sumber daya menggunakan subnet. IPv6-only Resolusi DNS harus **IN_VPC** untuk melampirkan konfigurasi sumber daya CIDR ke gateway sumber daya.

Membuat gateway sumber daya di VPC Lattice

Gunakan konsol untuk membuat gateway sumber daya.

Untuk membuat gateway sumber daya menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Gerbang sumber daya.
3. Pilih Buat gateway sumber daya.
4. Masukkan nama yang unik dalam AWS akun Anda.
5. Pilih jenis alamat IP untuk gateway sumber daya.
6. Untuk jenis alamat IP, pilih jenis alamat IP untuk gateway sumber daya.
 - Jika Anda memilih IPv4 atau Dualstack untuk jenis alamat IP, Anda dapat memasukkan jumlah alamat IPv4 per ENI untuk gateway sumber daya Anda.

Defaultnya adalah 16 alamat IPv4 per ENI. Ini adalah jumlah IP yang cocok untuk membentuk koneksi dengan sumber daya backend Anda.
7. Pilih VPC tempat sumber daya berada.
8. Untuk grup keamanan, pilih hingga lima grup keamanan untuk mengontrol lalu lintas masuk dari VPC ke jaringan layanan.
9. Untuk Resolusi DNS Konfigurasi Sumber Daya, pilih bagaimana Anda ingin DNS diselesaikan untuk target nama domain.
 - Jika Anda menggunakan server DNS pribadi atau target nama domain Anda berada di zona host pribadi Route 53, setelah resolusi DNS ke IN_VPC.
10. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
11. Pilih Buat gateway sumber daya.

Untuk membuat gateway sumber daya menggunakan AWS CLI

Gunakan perintah [create-resource-gateway](#).

Menghapus gateway sumber daya di VPC Lattice

Gunakan konsol untuk menghapus gateway sumber daya.

Untuk menghapus gateway sumber daya menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.

2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Gerbang sumber daya.
3. Pilih kotak centang untuk gateway sumber daya yang ingin Anda hapus dan pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **confirm**, lalu pilih Hapus.

Untuk menghapus gateway sumber daya menggunakan AWS CLI

Gunakan perintah [delete-resource-gateway](#).

Identitas dan manajemen akses untuk AWS PrivateLink

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS PrivateLink IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Daftar Isi

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS PrivateLink bekerja dengan IAM](#)
- [Identity-based contoh kebijakan untuk AWS PrivateLink](#)
- [Kontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir](#)
- [AWS kebijakan terkelola untuk AWS PrivateLink](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS PrivateLink

Pengguna layanan — Jika Anda menggunakan AWS PrivateLink layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS PrivateLink fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda.

Administrator layanan — Jika Anda bertanggung jawab atas AWS PrivateLink sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS PrivateLink. Tugas Anda adalah menentukan AWS PrivateLink fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda sebaiknya mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke AWS PrivateLink.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk

informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh

identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana AWS PrivateLink bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS PrivateLink, pelajari fitur IAM yang tersedia untuk digunakan. AWS PrivateLink

Fitur IAM	AWS PrivateLink dukungan
Identity-based kebijakan	Ya
Resource-based kebijakan	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Service-linked peran	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS PrivateLink dan Layanan AWS pekerjaan lainnya dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Identity-based kebijakan untuk AWS PrivateLink

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk AWS PrivateLink

Untuk melihat contoh kebijakan AWS PrivateLink berbasis identitas, lihat. [Identity-based contoh kebijakan untuk AWS PrivateLink](#)

Resource-based kebijakan dalam AWS PrivateLink

Mendukung kebijakan berbasis sumber daya: Ya

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

AWS PrivateLink Layanan mendukung satu jenis kebijakan berbasis sumber daya, yang dikenal sebagai kebijakan titik akhir. Kebijakan endpoint mengontrol AWS prinsipal mana yang dapat

menggunakan endpoint untuk mengakses layanan endpoint. Untuk informasi selengkapnya, lihat [the section called “Kebijakan titik akhir”](#).

Tindakan kebijakan untuk AWS PrivateLink

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan di namespace `ec2`

Beberapa tindakan untuk AWS PrivateLink adalah bagian dari Amazon EC2 API. Tindakan kebijakan ini menggunakan `ec2` awalan. Untuk informasi selengkapnya, lihat [AWS PrivateLink tindakan](#) di Referensi API Amazon EC2.

Tindakan di namespace `vpce`

AWS PrivateLink juga menyediakan tindakan `AllowMultiRegion` hanya izin. Tindakan kebijakan ini menggunakan `vpce` awalan.

Sumber daya kebijakan untuk AWS PrivateLink

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"

```

Kunci kondisi kebijakan untuk AWS PrivateLink

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Kunci kondisi berikut khusus untuk AWS PrivateLink:

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

Untuk informasi selengkapnya, lihat [Kunci kondisi untuk Amazon EC2](#).

ACL di AWS PrivateLink

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan AWS PrivateLink

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya

IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

Menggunakan kredensial sementara dengan AWS PrivateLink

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

Cross-service izin utama untuk AWS PrivateLink

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

Peran layanan untuk AWS PrivateLink

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Service-linked peran untuk AWS PrivateLink

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Identity-based contoh kebijakan untuk AWS PrivateLink

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya AWS PrivateLink . Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) di Panduan Pengguna IAM](#).

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS PrivateLink, termasuk format ARN untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Amazon EC2](#) di Referensi Otorisasi Layanan.

Contoh

- [Kontrol penggunaan titik akhir VPC](#)
- [Kontrol pembuatan titik akhir VPC berdasarkan pemilik layanan](#)
- [Kontrol nama DNS pribadi yang dapat ditentukan untuk layanan titik akhir VPC](#)
- [Kontrol nama layanan yang dapat ditentukan untuk layanan titik akhir VPC](#)

Kontrol penggunaan titik akhir VPC

Secara default, pengguna tidak memiliki izin untuk bekerja dengan titik akhir. Anda dapat membuat kebijakan berbasis identitas yang memberikan izin kepada pengguna untuk membuat, memodifikasi, mendeskripsikan, dan menghapus titik akhir. Berikut adalah contohnya.

JSON

```
{  
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Action": "ec2:*VpcEndpoint*",
        "Resource": "*"
      }
    ]
  }
}

```

Untuk informasi tentang mengontrol akses ke layanan menggunakan titik akhir VPC, lihat [the section called “Kebijakan titik akhir”](#)

Kontrol pembuatan titik akhir VPC berdasarkan pemilik layanan

Anda dapat menggunakan tombol `ec2:VpceServiceOwner` kondisi untuk mengontrol titik akhir VPC apa yang dapat dibuat berdasarkan siapa yang memiliki layanan (`amazon`, `aws-marketplace`, atau ID akun). Contoh berikut memberikan izin untuk membuat titik akhir VPC dengan pemilik layanan yang ditentukan. Untuk menggunakan contoh ini, ganti Wilayah, ID akun, dan pemilik layanan.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc/*",
        "arn:aws:ec2:us-east-1:111111111111:security-group/*",
        "arn:aws:ec2:us-east-1:111111111111:subnet/*",
        "arn:aws:ec2:us-east-1:111111111111:route-table/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
      ]
    }
  ]
}

```

```

        "Condition": {
            "StringEquals": {
                "ec2:VpceServiceOwner": [
                    "amazon"
                ]
            }
        }
    ]
}

```

Kontrol nama DNS pribadi yang dapat ditentukan untuk layanan titik akhir VPC

Anda dapat menggunakan tombol `ec2:VpceServicePrivateDnsName` kondisi untuk mengontrol layanan titik akhir VPC apa yang dapat dimodifikasi atau dibuat berdasarkan nama DNS pribadi yang terkait dengan layanan titik akhir VPC. Contoh berikut memberikan izin untuk membuat layanan titik akhir VPC dengan nama DNS pribadi yang ditentukan. Untuk menggunakan contoh ini, ganti Region, ID akun, dan nama DNS pribadi.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}

```

```

    }
  }
]
}

```

Kontrol nama layanan yang dapat ditentukan untuk layanan titik akhir VPC

Anda dapat menggunakan tombol `ec2:VpceServiceName` kondisi untuk mengontrol titik akhir VPC apa yang dapat dibuat berdasarkan nama layanan titik akhir VPC. Contoh berikut memberikan izin untuk membuat titik akhir VPC dengan nama layanan yang ditentukan. Untuk menggunakan contoh ini, ganti Region, ID akun, dan nama layanan.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc/*",
        "arn:aws:ec2:us-east-1:111111111111:security-group/*",
        "arn:aws:ec2:us-east-1:111111111111:subnet/*",
        "arn:aws:ec2:us-east-1:111111111111:route-table/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:VpceServiceName": [
            "com.amazonaws.111111111111.s3"
          ]
        }
      }
    }
  ]
}

```

```
} ]
```

Kontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir

Kebijakan endpoint adalah kebijakan berbasis sumber daya yang Anda lampirkan ke titik akhir VPC untuk mengontrol AWS prinsipal mana yang dapat menggunakan titik akhir untuk mengakses Layanan AWS.

Kebijakan endpoint tidak mengesampingkan atau mengganti kebijakan berbasis identitas atau kebijakan berbasis sumber daya. Misalnya, jika Anda menggunakan titik akhir antarmuka untuk terhubung ke Amazon S3, Anda juga dapat menggunakan kebijakan bucket Amazon S3 untuk mengontrol akses ke bucket dari titik akhir tertentu atau VPC tertentu.

Daftar Isi

- [Pertimbangan-pertimbangan](#)
- [Kebijakan titik akhir default](#)
- [Kebijakan untuk titik akhir antarmuka](#)
- [Prinsip untuk titik akhir gateway](#)
- [Memperbarui kebijakan titik akhir VPC](#)

Pertimbangan-pertimbangan

- Kebijakan endpoint adalah dokumen kebijakan JSON yang menggunakan bahasa kebijakan IAM. Itu harus mengandung elemen [Principal](#). Ukuran kebijakan endpoint tidak boleh melebihi 20.480 karakter, termasuk spasi putih.
- Saat membuat antarmuka atau titik akhir gateway untuk sebuah Layanan AWS, Anda dapat melampirkan kebijakan titik akhir tunggal ke titik akhir. Anda dapat [memperbarui kebijakan endpoint](#) kapan saja. Jika Anda tidak melampirkan kebijakan endpoint, kami melampirkan kebijakan [endpoint default](#).
- Tidak semua Layanan AWS mendukung kebijakan titik akhir. Jika Layanan AWS tidak mendukung kebijakan titik akhir, kami mengizinkan akses penuh ke titik akhir apa pun untuk layanan. Untuk informasi selengkapnya, lihat [the section called “Lihat dukungan kebijakan titik akhir”](#).
- Saat Anda membuat titik akhir VPC untuk layanan endpoint selain layanan Layanan AWS, kami mengizinkan akses penuh ke titik akhir.

- Anda tidak dapat menggunakan karakter wildcard (* atau?) atau [operator kondisi numerik](#) dengan kunci konteks global yang mereferensikan pengidentifikasi yang dihasilkan sistem (misalnya, atau).
aws:PrincipalAccount aws:SourceVpc
- Bila Anda menggunakan [operator kondisi string](#), Anda harus menggunakan setidaknya enam karakter berturut-turut sebelum atau setelah setiap karakter wildcard.
- Saat Anda menentukan ARN dalam elemen sumber daya atau kondisi, bagian akun ARN dapat menyertakan ID akun atau karakter wildcard, tetapi tidak keduanya.
- Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan.

Kebijakan titik akhir default

Kebijakan endpoint default memberikan akses penuh ke titik akhir.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Kebijakan untuk titik akhir antarmuka

Misalnya kebijakan titik akhir untuk Layanan AWS, lihat [the section called “Layanan yang terintegrasi”](#). Kolom pertama dalam tabel berisi tautan ke AWS PrivateLink dokumentasi untuk masing-masing Layanan AWS. Jika Layanan AWS mendukung kebijakan titik akhir, dokumentasinya menyertakan contoh kebijakan titik akhir.

Prinsip untuk titik akhir gateway

Dengan titik akhir gateway, Principal elemen harus diatur ke*. Untuk menentukan prinsipal, gunakan tombol aws:PrincipalArn kondisi.

```
"Condition": {
```

```
"StringEquals": {  
    "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"  
}  
}
```

Jika Anda menentukan prinsipal dalam format berikut, akses diberikan kepada Pengguna root akun AWS satu-satunya, tidak semua pengguna dan peran untuk akun.

```
"AWS": "account_id"
```

Misalnya kebijakan titik akhir untuk titik akhir gateway, lihat berikut ini:

- [Titik akhir untuk Amazon S3](#)
- [Titik akhir untuk DynamoDB](#)

Memperbarui kebijakan titik akhir VPC

Gunakan prosedur berikut untuk memperbarui kebijakan titik akhir untuk. Layanan AWS Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan.

Untuk memperbarui kebijakan titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir VPC.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan kustom.
6. Pilih Simpan.

Untuk memperbarui kebijakan titik akhir menggunakan baris perintah

- [memodifikasi-vpc-titik akhir](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#) (Alat untuk Windows PowerShell)

AWS kebijakan terkelola untuk AWS PrivateLink

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS PrivateLink pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS PrivateLink sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS PrivateLink dokumen.

Ubah	Deskripsi	Date
AWS PrivateLink mulai melacak perubahan	AWS PrivateLink mulai melacak perubahan untuk kebijakan AWS terkelolanya.	1 Maret 2021

CloudWatch metrik untuk AWS PrivateLink

AWS PrivateLink menerbitkan titik data ke Amazon CloudWatch untuk titik akhir antarmuka Anda, titik akhir Load Balancer Gateway, dan layanan titik akhir. CloudWatch memungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anggap metrik sebagai variabel untuk memantau, dan titik data sebagai nilai variabel tersebut dari waktu ke waktu. Setiap titik data memiliki timestamp terkait dan pengukuran unit 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.

Metrik diterbitkan untuk semua titik akhir antarmuka, titik akhir Load Balancer Gateway, dan layanan titik akhir. Mereka tidak dipublikasikan untuk titik akhir gateway atau untuk konsumen layanan titik akhir yang menggunakan akses lintas wilayah. Secara default, AWS PrivateLink kirimkan metrik ke CloudWatch dalam interval satu menit, tanpa biaya tambahan.

Untuk informasi selengkapnya, lihat [Panduan CloudWatch Pengguna Amazon](#).

Daftar Isi

- [Metrik dan dimensi titik akhir](#)
- [Metrik dan dimensi layanan titik akhir](#)
- [Lihat CloudWatch metrik](#)
- [Gunakan aturan Wawasan Kontributor bawaan](#)

Metrik dan dimensi titik akhir

AWS/PrivateLinkEndpointsNamespace menyertakan metrik berikut untuk titik akhir antarmuka dan titik akhir Gateway Load Balancer.

Metrik	Deskripsi
ActiveConnections	Jumlah koneksi aktif bersamaan. Ini termasuk koneksi dalam status SYN_SENT dan DESIGN.

Metrik	Deskripsi
	<p>Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit.</p> <p>Statistics: Statistik yang paling berguna adalah Average, Maximum, dan Minimum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
BytesProcessed	<p>Jumlah byte yang dipertukarkan antara titik akhir dan layanan titik akhir, digabungkan di kedua arah. Ini adalah jumlah byte yang ditagih ke pemilik titik akhir. Tagihan menampilkan nilai ini dalam GB.</p> <p>Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit.</p> <p>Statistik: Statistik yang paling berguna adalah Average, Sum, Maximum, dan Minimum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

Metrik	Deskripsi
NewConnections	<p>Jumlah koneksi baru yang dibuat melalui titik akhir.</p> <p>Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit.</p> <p>Statistik: Statistik yang paling berguna adalah Average, Sum, Maximum, dan Minimum.</p> <p>Dimensi</p> <ul style="list-style-type: none">• Endpoint Type, Service Name, VPC Endpoint Id, VPC Id• Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
PacketsDropped	<p>Jumlah paket yang dijatuhkan oleh titik akhir. Metrik ini mungkin tidak menangkap semua drop paket. Peningkatan nilai dapat menunjukkan bahwa layanan endpoint atau endpoint tidak sehat.</p> <p>Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit.</p> <p>Statistics: Statistik yang paling berguna adalah Average, Sum, dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none">• Endpoint Type, Service Name, VPC Endpoint Id, VPC Id• Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

Metrik	Deskripsi
RstPacketsReceived	<p>Jumlah paket RST yang diterima oleh endpoint. Peningkatan nilai dapat menunjukkan bahwa layanan endpoint tidak sehat.</p> <p>Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit.</p> <p>Statistics: Statistik yang paling berguna adalah Average, Sum, dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> Endpoint Type, Service Name, VPC Endpoint Id, VPC Id Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

Untuk memfilter metrik ini, gunakan dimensi berikut.

Dimensi	Deskripsi
Endpoint Type	Memfilter data metrik berdasarkan tipe titik akhir (Interface GatewayLoadBalancer).
Service Name	Memfilter data metrik berdasarkan nama layanan.
Subnet Id	Filter data metrik dengan subnet.
VPC Endpoint Id	Memfilter data metrik berdasarkan titik akhir VPC.
VPC Id	Memfilter data metrik oleh VPC.

Metrik dan dimensi layanan titik akhir

AWS/PrivateLinkServicesNamespace menyertakan metrik berikut untuk layanan titik akhir.

Metrik	Deskripsi
ActiveConnections	<p>Jumlah maksimum koneksi aktif dari klien ke target melalui titik akhir. Peningkatan nilai dapat menunjukkan perlunya menambahkan target ke penyeimbang beban.</p> <p>Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit.</p> <p>Statistik: Statistik yang paling berguna adalah Average dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
BytesProcessed	<p>Jumlah byte yang dipertukarkan antara layanan endpoint dan endpoint, di kedua arah.</p> <p>Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit.</p> <p>Statistics: Statistik yang paling berguna adalah Average, Sum, dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
EndpointsCount	Jumlah titik akhir yang terhubung ke layanan endpoint.

Metrik	Deskripsi
	<p>Kriteria pelaporan: Ada nilai bukan nol selama periode lima menit.</p> <p>Statistik: Statistik yang paling berguna adalah Average dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> • Service Id
NewConnections	<p>Jumlah koneksi baru yang dibuat dari klien ke target melalui titik akhir. Peningkatan nilai dapat menunjukkan perlunya menambahkan target ke penyeimbang beban.</p> <p>Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit.</p> <p>Statistics: Statistik yang paling berguna adalah Average, Sum, dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none"> • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

Metrik	Deskripsi
RstPacketsSent	<p>Jumlah paket RST yang dikirim ke endpoint oleh layanan endpoint. Peningkatan nilai dapat menunjukkan bahwa ada target yang tidak sehat.</p> <p>Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit.</p> <p>Statistics: Statistik yang paling berguna adalah Average, Sum, dan Maximum.</p> <p>Dimensi</p> <ul style="list-style-type: none">• Service Id• Az, Service Id• Load Balancer Arn, Service Id• Az, Load Balancer Arn, Service Id• Service Id, VPC Endpoint Id

Untuk memfilter metrik ini, gunakan dimensi berikut.

Dimensi	Deskripsi
Az	Memfilter data metrik berdasarkan Availability Zone.
Load Balancer Arn	Memfilter data metrik berdasarkan penyeimbang beban.
Service Id	Memfilter data metrik berdasarkan layanan titik akhir.
VPC Endpoint Id	Memfilter data metrik berdasarkan titik akhir VPC.

Lihat CloudWatch metrik

Anda dapat melihat CloudWatch metrik ini menggunakan konsol VPC Amazon, konsol, atau CloudWatch sebagai AWS CLI berikut.

Untuk melihat metrik menggunakan konsol VPC Amazon

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Titik akhir. Pilih titik akhir Anda dan kemudian pilih tab Monitoring.
3. Di panel navigasi, pilih Layanan titik akhir. Pilih layanan endpoint Anda dan kemudian pilih tab Monitoring.

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 AWS/PrivateLinkEndpointsnamespace.
4. Pilih AWS/PrivateLinkServicesnamespace.

Untuk melihat metrik menggunakan AWS CLI

Gunakan perintah [daftar-metrik berikut untuk mencantumkan metrik](#) yang tersedia untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway:

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

Gunakan perintah [list-metrics berikut untuk mencantumkan metrik](#) yang tersedia untuk layanan endpoint:

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

Gunakan aturan Wawasan Kontributor bawaan

AWS PrivateLink menyediakan aturan Contributor Insights bawaan untuk layanan endpoint Anda guna membantu Anda menemukan titik akhir mana yang merupakan kontributor terbesar untuk setiap metrik yang didukung. Untuk informasi selengkapnya, lihat [Wawasan Kontributor](#) di CloudWatch Panduan Pengguna Amazon.

AWS PrivateLink memberikan aturan berikut:

- VpcEndpointService-ActiveConnectionsByEndpointId-v1— Memberi peringkat titik akhir berdasarkan jumlah koneksi aktif.

- `VpcEndpointService-BytesByEndpointId-v1`— Peringkat titik akhir dengan jumlah byte yang diproses.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`— Peringkat titik akhir dengan jumlah koneksi baru.
- `VpcEndpointService-RstPacketsByEndpointId-v1`— Peringkat titik akhir dengan jumlah paket RST yang dikirim ke titik akhir.

Sebelum Anda dapat menggunakan aturan bawaan, Anda harus mengaktifkannya. Setelah Anda mengaktifkan aturan, aturan mulai mengumpulkan data kontributor. Untuk informasi tentang biaya untuk Wawasan Kontributor, lihat Harga [Amazon CloudWatch](#).

Anda harus memiliki izin berikut untuk menggunakan Contributor Insights:

- `cloudwatch:DeleteInsightRules`— Untuk menghapus aturan Contributor Insights.
- `cloudwatch:DisableInsightRules`— Untuk menonaktifkan aturan Contributor Insights.
- `cloudwatch:GetInsightRuleReport`— Untuk mendapatkan datanya.
- `cloudwatch:ListManagedInsightRules`— Untuk mencantumkan aturan Contributor Insights yang tersedia.
- `cloudwatch:PutManagedInsightRules`— Untuk mengaktifkan aturan Contributor Insights.

Tugas

- [Aktifkan aturan Contributor Insights](#)
- [Nonaktifkan aturan Wawasan Kontributor](#)
- [Hapus aturan Wawasan Kontributor](#)

Aktifkan aturan Contributor Insights

Gunakan prosedur berikut untuk mengaktifkan aturan bawaan untuk AWS PrivateLink menggunakan salah satu Konsol Manajemen AWS atau AWS CLI.

Untuk mengaktifkan aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint Anda.

4. Pada tab Contributor Insights, pilih Aktifkan.
5. (Opsional) Secara default, semua aturan diaktifkan. Untuk mengaktifkan hanya aturan tertentu, pilih aturan yang tidak boleh diaktifkan dan kemudian pilih Tindakan, Nonaktifkan aturan. Ketika diminta konfirmasi, pilih Nonaktifkan.

Untuk mengaktifkan aturan Contributor Insights untuk menggunakan AWS PrivateLink AWS CLI

1. Gunakan perintah [list-managed-insight-rules sebagai berikut untuk menghitung aturan](#) yang tersedia. Untuk `--resource-arn` opsi, tentukan ARN dari layanan endpoint Anda.

```
aws cloudwatch list-managed-insight-rules --resource-arn
arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Dalam output `list-managed-insight-rules` perintah, salin nama template dari `TemplateName` bidang. Berikut ini adalah contoh dari bidang ini.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Gunakan perintah [put-managed-insight-rules sebagai berikut untuk mengaktifkan aturan](#). Anda harus menentukan nama template dan ARN dari layanan endpoint Anda.

```
aws cloudwatch put-managed-insight-rules --managed-rules
TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Nonaktifkan aturan Wawasan Kontributor

Anda dapat menonaktifkan aturan bawaan AWS PrivateLink kapan saja. Setelah Anda menonaktifkan aturan, aturan berhenti mengumpulkan data kontributor, tetapi data kontributor yang ada disimpan hingga berusia 15 hari. Setelah Anda menonaktifkan aturan, Anda dapat mengaktifkannya lagi untuk melanjutkan pengumpulan data kontributor.

Untuk menonaktifkan aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint Anda.

4. Pada tab Contributor Insights, pilih Nonaktifkan semua untuk menonaktifkan semua aturan. Atau, perluas panel Aturan, pilih aturan yang akan dinonaktifkan, lalu pilih Tindakan, Nonaktifkan aturan
5. Ketika dimintai konfirmasi, pilih Nonaktifkan.

Untuk menonaktifkan aturan Contributor Insights untuk menggunakan AWS PrivateLink AWS CLI

Gunakan perintah [disable-insight-rules untuk menonaktifkan aturan](#).

Hapus aturan Wawasan Kontributor

Gunakan prosedur berikut untuk menghapus aturan bawaan untuk AWS PrivateLink menggunakan salah satu Konsol Manajemen AWS atau AWS CLI. Setelah Anda menghapus aturan, aturan berhenti mengumpulkan data kontributor dan kami menghapus data kontributor yang ada.

Untuk menghapus aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada panel navigasi, silakan pilih Wawasan Wawasan Kontributor.
3. Perluas panel Aturan dan pilih aturan.
4. Pilih Tindakan, Hapus aturan.
5. Saat diminta konfirmasi, pilih Hapus.

Untuk menghapus aturan Contributor Insights untuk menggunakan AWS PrivateLink AWS CLI

Gunakan perintah [delete-insight-rules untuk menghapus aturan](#).

AWS PrivateLink kuota

AWS Akun Anda memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota adalah Region-specific. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan. Jika Anda meminta penambahan kuota yang berlaku per sumber daya, kami meningkatkan kuota untuk semua sumber daya di Wilayah.

Untuk meminta penambahan kuota, lihat [Meminta penambahan kuota](#) di Panduan Pengguna Service Quotas.

Permintaan throttling

Tindakan API untuk AWS PrivateLink adalah bagian dari Amazon EC2 API. Amazon EC2 membatasi permintaan API-nya di level tersebut. Akun AWS Untuk informasi selengkapnya, lihat [Meminta pembatasan di Panduan](#) Pengembang Amazon EC2. Selain itu, permintaan API juga dibatasi di tingkat organisasi untuk membantu kinerja. AWS PrivateLink Jika Anda menggunakan AWS Organizations dan menerima kode RequestLimitExceeded kesalahan saat Anda masih dalam batas API tingkat akun, lihat [Cara mengidentifikasi AWS akun yang melakukan banyak panggilan API](#). Jika Anda memerlukan bantuan, hubungi tim akun Anda atau buka kasus dukungan teknis menggunakan layanan VPC dan kategori Titik Akhir VPC. Pastikan untuk melampirkan gambar kode RequestLimitExceeded kesalahan.

Kuota titik akhir VPC

AWS Akun Anda memiliki kuota berikut yang terkait dengan titik akhir VPC.

Nama	Default	Dapat disesuaikan	Komentar
Titik akhir antara muka dan Penyeimbang Beban Gateway per VPC	50	Ya	Ini adalah kuota gabungan untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway
Titik akhir VPC Gateway per Wilayah	20	Ya	Anda dapat membuat hingga 255 titik akhir gateway per VPC

Nama	Default	Dapat disesuaikan	Komentar
Sumber daya VPC endpoint untuk VPC	200	Ya	
Layanan jaringan VPC endpoint untuk VPC	50	Ya	
Karakter per kebijakan VPC endpoint	20,480	Tidak	Ukuran maksimum kebijakan titik akhir VPC, termasuk spasi putih

Pertimbangan berikut berlaku untuk lalu lintas yang melewati titik akhir VPC:

- Secara default, setiap titik akhir VPC dapat mendukung bandwidth hingga 10 Gbps per Availability Zone, dan secara otomatis menskalakan hingga 100 Gbps. Bandwidth maksimum untuk titik akhir VPC, saat mendistribusikan beban di semua Availability Zone, adalah jumlah Availability Zone dikalikan dengan 100 Gbps. Jika aplikasi Anda membutuhkan throughput yang lebih tinggi, hubungi AWS dukungan.
- Unit transmisi maksimum (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang diizinkan yang dapat dilewatkan melalui titik akhir VPC. Semakin besar MTU, semakin banyak data yang dapat dilewatkan dalam satu paket tunggal. VPC endpoint mendukung MTU 8500 byte. Paket dengan ukuran lebih besar dari 8500 byte yang tiba di VPC endpoint akan dijatuhkan.
- Path MTU Discovery (PMTUD) tidak didukung. Titik akhir VPC tidak menghasilkan pesan ICMP berikut: Destination Unreachable: Fragmentation needed and Don't Fragment was Set (Tipe 3, Kode 4).
- Titik akhir VPC memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi lebih lanjut, lihat [RFC879](#).

Riwayat dokumen untuk AWS PrivateLink

Tabel berikut menjelaskan rilis untuk AWS PrivateLink.

Perubahan	Deskripsi	Tanggal
Akses sumber daya dan jaringan layanan	AWS PrivateLink mendukung akses sumber daya dan jaringan layanan di seluruh VPC dan batas akun.	Desember 1, 2024
Cross-Region akses	Penyedia layanan dapat meng-host layanan di satu Wilayah dan membuatnya tersedia dalam satu set AWS Wilayah. Konsumen layanan memilih Wilayah layanan saat membuat titik akhir.	November 26, 2024
Alamat IP yang ditunjuk	Anda dapat menentukan alamat IP untuk antarmuka jaringan titik akhir Anda saat membuat atau memodifikasi titik akhir VPC Anda.	17 Agustus 2023
Dukungan IPv6	Anda dapat mengonfigurasi layanan titik akhir Load Balancer Gateway dan titik akhir Load Balancer Gateway untuk mendukung alamat IPv4 dan IPv6 atau hanya alamat IPv6.	12 Desember 2022
Wawasan Kontributor	Anda dapat menggunakan aturan Contributor Insights bawaan untuk mengidentifikasi titik akhir tertentu	18 Agustus 2022

yang merupakan kontributor teratas untuk metrik tersebut. CloudWatch AWS PrivateLink

[Dukungan IPv6](#)

Penyedia layanan dapat mengaktifkan layanan endpoint mereka untuk menerima permintaan IPv6, bahkan jika layanan backend mereka hanya mendukung IPv4. Jika layanan endpoint menerima permintaan IPv6, konsumen layanan dapat mengaktifkan dukungan IPv6 untuk titik akhir antarmuka mereka sehingga mereka dapat mengakses layanan endpoint melalui IPv6.

Mei 11, 2022

[CloudWatch metrik](#)

AWS PrivateLink menerbitkan CloudWatch metrik untuk titik akhir antarmuka Anda, titik akhir Load Balancer Gateway, dan layanan titik akhir.

27 Januari 2022

[Titik akhir Load Balancer Gateway](#)

Anda dapat membuat endpoint Gateway Load Balancer di VPC Anda untuk mengarahkan lalu lintas ke layanan VPC endpoint yang Anda konfigurasi menggunakan Gateway Load Balancer.

10 November 2020

Kebijakan titik akhir VPC	Anda dapat melampirkan kebijakan IAM ke titik akhir VPC antarmuka untuk layanan untuk AWS mengontrol akses ke layanan.	23 Maret 2020
Kunci kondisi untuk titik akhir VPC dan layanan titik akhir	Anda dapat menggunakan tombol kondisi EC2 untuk mengontrol akses ke titik akhir VPC dan layanan titik akhir.	6 Maret 2020
Menandai titik akhir VPC dan layanan endpoint pada pembuatan	Anda dapat menambahkan tag saat membuat titik akhir VPC dan layanan titik akhir.	5 Februari 2020
Nama DNS pribadi	Anda dapat mengakses layanan AWS PrivateLink berbasis dari dalam VPC Anda menggunakan nama DNS pribadi.	6 Januari 2020
Layanan titik akhir VPC	Anda dapat membuat layanan titik akhir Anda sendiri dan memungkinkan orang lain Akun AWS dan pengguna untuk terhubung ke layanan Anda melalui titik akhir VPC antarmuka. Anda dapat menawarkan layanan endpoint Anda untuk berlangganan di AWS Marketplace	28 November 2017

[Antarmuka titik akhir VPC
untuk Layanan AWS](#)

Anda dapat membuat titik akhir antarmuka untuk terhubung ke Layanan AWS yang terintegrasi dengan AWS PrivateLink tanpa menggunakan gateway internet atau perangkat NAT.

8 November 2017

[Titik akhir VPC untuk
DynamoDB](#)

Anda dapat membuat titik akhir VPC gateway untuk mengakses Amazon DynamoDB dari VPC Anda tanpa menggunakan gateway internet atau perangkat NAT.

16 Agustus 2017

[Titik akhir VPC untuk Amazon
S3](#)

Anda dapat membuat titik akhir VPC gateway untuk mengakses Amazon S3 dari VPC Anda tanpa menggunakan gateway internet atau perangkat NAT.

11 Mei 2015

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