



Panduan Developerr

Amazon Route 53



Versi API 2013-04-01

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

Amazon Route 53: Panduan Developerr

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 antara para pelanggan, atau dengan cara apa pun yang menghina 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 Amazon Route 53?	1
Cara kerja pendaftaran domain	3
Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda	4
Ikhtisar tentang cara Anda mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas internet untuk domain Anda	5
Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda	6
Bagaimana Amazon Route 53 memeriksa kondisi sumber daya Anda	8
Konsep Amazon Route 53	10
Konsep pendaftaran domain	11
Konsep Sistem Nama Domain (Domain Name System/DNS)	12
Konsep bidang kontrol dan data	18
Konsep pemeriksaan kondisi	19
Cara memulai Amazon Route 53	20
Mengakses Amazon Route 53	20
AWS Identity and Access Management	21
Harga dan penagihan Amazon Route 53	21
Bekerja dengan AWS SDKs	21
Memulai	23
Penyiapan	23
Mendaftar untuk Akun AWS	24
Buat pengguna dengan akses administratif	24
Unduh alat	25
Rutekan lalu lintas DNS ke situs web statis Amazon S3	26
Prasyarat	27
Langkah 1: Rutekan lalu lintas DNS untuk domain Anda ke bucket situs web Anda	27
Langkah 2: Uji situs web Anda	29
Rutekan lalu lintas DNS ke distribusi CloudFront	30
Prasyarat	30
Langkah 1: Rutekan lalu lintas DNS untuk domain Anda ke distribusi Anda CloudFront	31
Mengintegrasikan dengan layanan lain	34
Pencatatan, pemantauan, dan penandaan	34
Merutekan lalu lintas ke sumber daya lain AWS	35
Format nama domain DNS	38
Memformat nama domain untuk pendaftaran nama domain	38

Memformat nama domain untuk zona yang di-hosting dan catatan	38
Menggunakan tanda bintang (*) dalam nama zona yang di-hosting dan catatan	39
Memformat nama domain yang diinternasionalisasi	40
Mendaftarkan dan mengelola domain	43
Mendaftarkan domain baru	44
Mendaftarkan domain baru	44
Nilai yang Anda tentukan saat mendaftar atau mentransfer domain	51
Nilai yang dikembalikan Amazon Route 53 saat Anda mendaftar domain	58
Melihat status pendaftaran domain	59
Memperbarui pengaturan domain	60
Memperbarui informasi kontak dan kepemilikan domain	61
Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain	70
Mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain	74
Mengunci domain untuk mencegah transfer tidak sah ke registrar lain	75
Memperpanjang masa pendaftaran untuk domain	76
Memperbarui server nama untuk menggunakan registrar lain	78
Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain	79
Memperbarui pendaftaran untuk domain	83
Memulihkan domain yang kedaluwarsa atau dihapus	86
Mengganti zona yang di-hosting untuk domain	89
Mentransfer domain	90
Pilih jenis transfer Anda	91
Daftar pemeriksaan pra-transfer	93
Transfer ke Route 53	96
Masalah transfer umum	116
Transfer dari Route 53	118
Transfer ke AWS akun lain	124
Status transfer	128
Dampak transfer pada tanggal kedaluwarsa domain	131
Mengirim ulang email otorisasi dan konfirmasi	133
Memperbarui alamat email	134
Mengirim ulang email	134
Mengonfigurasi DNSSEC untuk domain	139
Gambaran umum tentang cara DNSSEC melindungi domain Anda	140
Prasyarat dan nilai maksimal untuk mengonfigurasi DNSSEC domain	142

Menambahkan kunci publik untuk domain	142
Menghapus kunci publik untuk domain	143
Menemukan registrar Anda	145
Melihat informasi tentang domain	145
Menghapus pendaftaran nama domain	147
Menghubungi AWS Support tentang masalah pendaftaran domain	150
Menghubungi AWS Support ketika Anda dapat masuk ke AWS akun Anda	151
Menghubungi AWS Support jika Anda tidak dapat masuk ke AWS akun	152
Mengunduh laporan penagihan domain	152
Domain yang dapat Anda daftarkan dengan Amazon Route 53	153
Indeks untuk domain tingkat atas yang didukung	155
Domain tingkat atas generik	158
Domain tingkat atas geografis	438
Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda	503
Membuat Route 53 menjadi layanan DNS untuk domain yang ada	504
Membuat Route 53 sebagai layanan DNS untuk domain yang sedang digunakan	504
Membuat Route 53 menjadi layanan DNS untuk domain yang tidak aktif	514
Mengonfigurasi perutean DNS untuk domain baru	518
Merutekan lalu lintas ke sumber daya	520
Merutekan lalu lintas untuk subdomain	521
Bekerja dengan zona yang di-hosting	527
Bekerja dengan zona yang di-hosting publik	528
Bekerja dengan zona yang di-hosting privat	560
Migrasi zona yang dihosting ke akun lain AWS	574
Bekerja dengan catatan	585
Memilih kebijakan perutean	586
Memilih antara catatan alias dan nonalias	612
Tipe data DNS yang didukung	616
Membuat catatan dengan menggunakan konsol Amazon Route 53	638
Izin set catatan sumber daya	640
Nilai yang Anda tentukan	641
Membuat catatan dengan mengimpor file zona	732
Mengedit catatan	736
Menghapus catatan	737
Mencantumkan catatan	738
Mengonfigurasi penandatanganan DNSSEC	740

Mengaktifkan penandatanganan DNSSEC dan membuat rantai kepercayaan	742
Menonaktifkan penandatanganan DNSSEC	752
Bekerja dengan kunci yang dikelola pelanggan	757
Bekerja dengan kunci penandatanganan kunci () KSKs	758
Kunci KMS dan manajemen ZSK di Route 53	761
Bukti DNSSEC tentang ketidakberadaan di Route 53	762
Memecahkan masalah penandatanganan DNSSEC	763
Menggunakan AWS Cloud Map untuk membuat catatan dan pemeriksaan kesehatan	764
Kendala dan perilaku DNS	765
Ukuran respons maksimum	765
Pemrosesan bagian otoritatif	765
Pemrosesan bagian tambahan	765
Topik terkait	765
Arus Lalu Lintas	766
Keuntungan Arus Lalu Lintas	766
Membuat dan mengelola kebijakan lalu lintas	768
Membuat kebijakan lalu lintas	768
Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas	771
Melihat peta yang menunjukkan efek pengaturan geoproximity	781
Membuat versi tambahan dari kebijakan lalu lintas	785
Membuat kebijakan lalu lintas dengan menggunakan dokumen JSON	788
Melihat versi kebijakan lalu lintas dan catatan kebijakan terkait	791
Menghapus versi kebijakan lalu lintas dan kebijakan lalu lintas	795
Membuat dan mengelola catatan kebijakan	798
Membuat catatan kebijakan	799
Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan	801
Memperbarui catatan kebijakan	803
Menghapus catatan kebijakan	805
Apa itu VPC Resolver?	807
Menyelesaikan kueri DNS antara VPCs dan jaringan Anda	809
Bagaimana kueri DNS dari jaringan Anda diteruskan ke VPC Resolver	813
Bagaimana titik akhir Resolver meneruskan kueri DNS dari Anda ke jaringan Anda VPCs ...	815
Pertimbangan saat membuat titik akhir masuk dan keluar	824
Ketersediaan dan penskalaan Route 53 VPC Resolver	828
Mulai menggunakan Route 53 VPC Resolver	830
Meneruskan kueri DNS masuk ke VPCs	832

Mengonfigurasi penerusan masuk	832
Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk	833
Mengelola titik akhir masuk	837
Meneruskan kueri DNS keluar ke jaringan Anda	839
Mengonfigurasi penerusan keluar	840
Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar	842
Nilai yang Anda tentukan ketika membuat atau mengedit aturan	845
Mengelola titik akhir keluar	847
Mengelola aturan penerusan	850
Tutorial aturan delegasi penyelesai	857
Langkah-langkah untuk delegasi keluar	858
Jenis delegasi	858
Mengaktifkan validasi DNSSEC	864
Merutekan lalu lintas internet ke sumber daya Anda AWS	866
API Amazon API Gateway	866
Prasyarat	867
Mengonfigurasi Route 53 untuk merutekan lalu lintas ke titik akhir API Gateway	868
CloudFront Distribusi Amazon	871
Prasyarat	873
Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke distribusi CloudFront	874
EC2 Contoh Amazon	876
Prasyarat	876
Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke instans Amazon EC2	877
Layanan Pelari Aplikasi	879
Prasyarat	880
Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke layanan App Runner	880
Global Accelerator	881
Prasyarat	882
Mengkonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke akselerator	882
AWS Elastic Beanstalk lingkungan	884
Men-deploy aplikasi ke lingkungan Elastic Beanstalk	884
Mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda	884
Membuat catatan Route 53	885
penyeimbang beban ELB	888
Prasyarat	889

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke penyeimbang beban	
ELB	889
Bucket Amazon S3	891
Prasyarat	892
Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke Bucket S3	893
Titik akhir antarmuka Amazon Virtual Private Cloud	895
Prasyarat	895
Titik akhir antarmuka Amazon VPC	896
Amazon WorkMail	898
OpenSearch Layanan Amazon	900
Prasyarat	901
Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir domain	
OpenSearch Layanan Amazon	901
Kisi VPC	902
Prasyarat	903
Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir domain layanan	
VPC Lattice	903
AWS Sumber daya lainnya	904
Membuat pemeriksaan kondisi	906
Jenis pemeriksaan kondisi	907
Bagaimana Route 53 menentukan apakah pemeriksaan kondisi sehat	909
Bagaimana Route 53 menentukan status pemeriksaan kondisi yang memantau titik akhir ...	909
Bagaimana Route 53 menentukan status pemeriksaan kondisi yang memantau pemeriksaan kondisi lain	911
Bagaimana Route 53 menentukan status pemeriksaan kesehatan yang memantau CloudWatch alarm	911
Membuat, memperbarui, dan menghapus pemeriksaan kondisi	912
Membuat dan memperbarui pemeriksaan kondisi	913
Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi	916
Nilai yang ditampilkan Route 53 ketika Anda membuat pemeriksaan kondisi	942
Memperbarui pemeriksaan kesehatan saat Anda mengubah pengaturan CloudWatch alarm	942
Menonaktifkan atau mengaktifkan pemeriksaan kesehatan	944
Membalikkan pemeriksaan kesehatan	945
Menghapus pemeriksaan kondisi	945
Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi	947

Mengonfigurasi aturan router dan firewall untuk pemeriksaan kondisi	948
Mengonfigurasi failover DNS	949
Daftar tugas untuk mengonfigurasi failover DNS	950
Cara kerja pemeriksaan kondisi dalam konfigurasi yang sederhana	952
Cara kerja pemeriksaan kondisi dalam konfigurasi yang kompleks	956
Cara Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi	964
Failover active-active dan active-passive	967
Mengonfigurasi failover di zona yang di-hosting secara privat	970
Cara Route 53 mencegah masalah failover	971
Penamaan dan penandaan pemeriksaan kondisi	972
Pembatasan tanda	973
Menambahkan, mengedit, dan menghapus tanda untuk pemeriksaan kondisi	973
Menggunakan versi API sebelum 2012-12-12	976
Memantau status pemeriksaan kondisi dan mendapatkan notifikasi	977
Melihat status pemeriksaan kondisi dan alasan kegagalan pemeriksaan kondisi	977
Memantau latensi antara pemeriksa kondisi dan titik akhir Anda	980
Memantau pemeriksaan kesehatan menggunakan CloudWatch	984
Lihat status pemeriksaan kesehatan Anda	984
Lihat alarm pemeriksaan kesehatan	988
Lihat metrik pemeriksaan kesehatan di konsol CloudWatch	990
Buat alarm dengan notifikasi SNS	991
Penyelesai DNS Firewall	995
Cara kerja Resolver DNS Firewall	996
Komponen dan pengaturan DNS Firewall	996
Bagaimana Resolver DNS Firewall menyaring kueri DNS	1000
Langkah-langkah tingkat tinggi untuk menggunakan DNS Firewall	1001
Menggunakan grup aturan DNS Firewall di beberapa Wilayah	1002
Ketersediaan wilayah untuk DNS Firewall	1002
Memulai dengan Resolver DNS Firewall	1004
Contoh taman berdingding DNS Firewall Resolver	1004
Contoh daftar blok Resolver DNS Firewall	1006
Grup aturan dan aturan DNS Firewall	1008
Pengaturan grup aturan di DNS Firewall	1009
Pengaturan aturan di DNS Firewall	1010
Aturan tindakan di DNS Firewall	1012
Mengelola grup aturan dan aturan di DNS Firewall	1013

Daftar domain DNS Firewall Resolver	1016
Daftar Domain Terkelola	1017
Mengelola daftar domain Anda sendiri	1022
DNS Firewall Advanced	1025
Mengonfigurasi pencatatan kueri untuk DNS Firewall	1026
Berbagi grup aturan di antara akun	1028
Mengaktifkan perlindungan DNS Firewall untuk VPC	1031
Mengelola asosiasi antara grup aturan VPC dan firewall	1032
Konfigurasi VPC DNS Firewall	1033
Apa itu Profil Amazon Route 53?	1035
Prioritas profil	1036
Ketersediaan profil	1036
Menggunakan Profil	1036
Buat Profil	1037
Asosiasi grup aturan DNS Firewall	1039
Kaitkan zona yang di-hosting privat	1041
Kaitkan aturan Resolver	1041
Kaitkan titik Akhir VPC	1042
Konfigurasi pencatatan kueri asosiasikan	1042
Edit konfigurasi Profil	1044
Rekanan VPCs	1046
Melihat dan memperbarui Profil	1047
Menghapus Profil	1049
Melihat dan memperbarui sumber daya yang terkait dengan Profil	1050
Memutuskan sumber daya	1052
Melihat VPCs terkait dengan Profil	1053
Memutus VPC	1055
Bekerja dengan Profil Route 53 bersama	1056
Memberikan izin untuk berbagi Profil Route 53	1057
Prasyarat untuk berbagi Profil Route 53	1057
Berbagi Profil Route 53	1058
Membatalkan berbagi Profil Route 53 bersama	1059
Mengidentifikasi Profil Route 53 bersama	1060
Tanggung jawab dan izin untuk Profil Route 53 bersama	1060
Tagihan dan pengukuran	1061
Kuota contoh	1061

Apa itu Amazon Route 53 di Outposts?	1062
Gambaran umum arsitektur	1063
Route 53 pada fitur Outposts	1063
Perilaku VPC Resolver saat AWS Outposts terputus dari VPC	1064
Memulai dengan VPC Resolver aktif AWS Outposts	1064
Membuat titik akhir masuk	1065
Nilai yang Anda tentukan saat membuat atau mengedit titik akhir masuk di Outpost	1066
Membuat titik akhir keluar	1068
Nilai yang Anda tentukan saat Anda membuat atau mengedit titik akhir keluar dalam AWS Outposts	1068
Membuat aturan penerusan untuk titik akhir keluar	1070
Mengelola Resolver di Outpost	1070
Mengedit Resolver di Outpost	1071
Melihat Resolver pada status Outpost	1071
Menghapus Resolver di Outpost	1072
Mengelola titik akhir masuk pada Resolver di Outpost	1073
Melihat dan mengedit titik akhir masuk	1073
Melihat status titik akhir masuk	1074
Menghapus titik akhir masuk	1075
Mengelola titik akhir keluar pada Resolver di Outpost	1076
Melihat dan mengedit titik akhir keluar	1076
Melihat status titik akhir keluar	1076
Menghapus titik akhir keluar	1078
Apa itu Global Resolver	1079
Mengapa Route 53 Global Resolver?	1080
Konsep dan terminologi	1080
DNS resolver untuk klien di lokasi lokal dan terpencil	1081
Autentikasi klien DNS	1081
Resolusi DNS lalu lintas terpisah	1082
Ketersediaan tinggi dan kehadiran global	1083
Resolusi dan penerusan DNS	1083
Pemfilteran DNS dan daftar domain	1084
Deteksi ancaman DNS tingkat lanjut	1085
Pencatatan dan pemantauan	1086
Cara kerjanya	1086
Apa yang terjadi ketika klien membuat kueri DNS	1087

Arsitektur anycast global	1087
Pemfilteran dan keamanan DNS	1088
Kasus penggunaan	1088
Layanan terkait	1090
Mengakses Resolver Global	1091
Didukung Wilayah AWS	1091
Menyiapkan akses akun	1092
Mendaftar untuk Akun AWS	24
Buat pengguna dengan akses administratif	24
Membuat kebijakan dan peran	1094
Pertimbangan jaringan	1095
Tutorial: Buat Resolver Global Route 53 pertama Anda	1096
Prasyarat	1096
Langkah 1: Buat resolver global	1096
Langkah 2: Buat tampilan DNS dan konfigurasi otentikasi	1097
Langkah 3: Konfigurasi aturan penyaringan DNS (opsional)	1097
Langkah 4: Uji konfigurasi Anda	1098
Langkah 5: Memantau aktivitas DNS	1098
Langkah 6: Bersihkan (opsional)	1098
Langkah selanjutnya	1099
Mengelola tampilan DNS	1099
Mengelola tampilan DNS	1099
Mengelola asosiasi zona yang dihosting pribadi	1101
Konfigurasi pengaturan untuk tampilan DNS	1102
Mengelola kontrol akses	1105
Metode kontrol akses	1105
Mengkonfigurasi sumber akses	1106
Mengelola token akses	1107
Praktik terbaik	1111
Mengamankan DNS	1112
Konfigurasi dan kelola aturan DNS Firewall	1112
Daftar Domain Terkelola	1117
Membangun daftar domain	1120
Perlindungan tingkat lanjut DNS Firewall	1121
Kelola kebijakan keamanan	1122
Mengkonfigurasi asosiasi yang dihosting pribadi	1123

Kelola asosiasi zona yang dihosting pribadi	1124
Memantau aktivitas DNS	1125
Dapatkan visibilitas DNS	1126
Konfigurasi pemantauan DNS	1131
Memecahkan masalah DNS	1132
Mendiagnosis masalah konektivitas	1132
Selesaikan masalah kinerja	1134
Memecahkan masalah konfigurasi	1135
Memecahkan masalah akses sumber daya internal	1137
Kuota	1137
Kuota lembut	1138
Kuota keras	1139
Menciptakan AWS CloudFormation sumber daya	1140
Route 53, VPC Resolver, dan template CloudFormation	1140
Praktik terbaik untuk Route 53 dan CloudFormation	1141
Memahami konsistensi akhirnya	1141
Pengurutan catatan DNS dan logis IDs	1142
Menangani kegagalan rollback	1143
Pelajari lebih lanjut tentang CloudFormation	1144
Contoh kode	1145
Route 53	1146
Hal-hal mendasar	1146
Registrasi domain Route 53	1175
Hal-hal mendasar	1176
Keamanan	1258
Perlindungan data	1259
Perlindungan dari catatan delegasi yang menggantung	1260
Manajemen identitas dan akses	1262
Mengautentikasi dengan identitas	1262
Kontrol akses	1264
Gambaran umum manajemen akses	1264
Menggunakan kebijakan IAM untuk Route 53	1272
Menggunakan Peran Terkait Layanan	1284
AWS kebijakan terkelola	1289
Ketentuan penggunaan	1304
Referensi izin API Route 53	1314

Pencatatan log dan pemantauan	1315
Validasi kepatuhan	1316
Ketahanan	1317
Keamanan infrastruktur	1318
Mengirim temuan ke Security Hub CSPM	1319
Cara kerja temuan di Security Hub CSPM	1319
Jenis temuan yang dikirim DNS Firewall	1320
Mencoba lagi saat CSPM Security Hub tidak tersedia	1320
Memperbarui temuan yang ada di Security Hub CSPM	1320
Temuan khas dari DNS Firewall	1320
Mengaktifkan dan mengonfigurasi integrasi	1323
Menghentikan pengiriman temuan ke Security Hub CSPM	1323
Memantau	1324
Pencatatan kueri DNS publik	1324
Mengonfigurasi pencatatan untuk kueri DNS	1325
Menggunakan Amazon CloudWatch untuk mengakses log kueri DNS	1327
Mengubah periode retensi untuk log dan mengekspor log ke Amazon S3	1328
Menghentikan pencatatan kueri	1328
Nilai-nilai yang muncul di log kueri DNS	1329
Contoh log kueri	1330
Pencatatan kueri Resolver	1330
Sumber daya yang dapat Anda kirim log kueri Resolver	1332
Mengelola konfigurasi	1334
Memantau pendaftaran domain	1343
Memantau sumber daya Anda dengan pemeriksaan kesehatan Amazon Route 53 dan Amazon CloudWatch	1343
Metrik dan dimensi untuk pemeriksaan kondisi	1343
Memantau zona yang dihosting menggunakan Amazon CloudWatch	1346
CloudWatch metrik untuk Route 53 zona yang dihosting publik	1346
CloudWatch dimensi untuk metrik zona yang dihosting publik Route 53	1348
Memantau Route 53 titik akhir VPC Resolver dengan Amazon CloudWatch	1348
Metrik dan dimensi untuk VPC Resolver	1349
Memantau grup aturan DNS Firewall Resolver dengan Amazon CloudWatch	1357
Metrik dan dimensi untuk Firewall DNS	1357
Mengelola acara DNS Firewall menggunakan EventBridge	1359
Acara Resolver DNS Firewall	1360

Mengirim acara DNS Firewall	1361
Izin	1363
Sumber daya tambahan	1364
Referensi detail Acara DNS Firewall	1364
Mencatat panggilan API Amazon Route 53 dengan AWS CloudTrail	1372
Informasi rute 53 di CloudTrail	1372
Melihat peristiwa Route 53 dalam riwayat peristiwa	1373
Memahami entri berkas log Route 53	1373
Pemecahan Masalah	1382
Domain saya tidak tersedia di internet	1383
Anda mendaftarkan domain baru, tetapi tidak mengeklik tautan di email konfirmasi	1384
Anda mentransfer pendaftaran domain ke Amazon Route 53, tetapi Anda tidak mentransfer layanan DNS	1384
Anda ditransfer pendaftaran domain dan menentukan server nama yang salah dalam pengaturan domain	1386
Anda mentransfer layanan DNS terlebih dahulu, tetapi Anda tidak menunggu cukup lama sebelum mentransfer pendaftaran domain	1387
Anda menghapus zona host yang digunakan Route 53 untuk merutekan lalu lintas internet untuk domain	1388
Domain Anda telah ditangguhkan	1389
Domain saya ditangguhkan (statusnya ClientHold)	1389
Anda mendaftarkan domain baru, tetapi tidak mengeklik tautan di email konfirmasi	1390
Anda menonaktifkan perpanjangan otomatis untuk domain, dan domain kedaluwarsa	1391
Anda mengubah alamat email untuk kontak pendaftar, tetapi Anda tidak memverifikasi bahwa alamat email baru itu valid	1391
Kami tidak dapat memproses pembayaran Anda untuk perpanjangan domain otomatis, dan domain kedaluwarsa	1392
Kami menangguhkan domain untuk pelanggaran Kebijakan Penggunaan yang Diterima AWS	1392
Kami menangguhkan domain karena perintah pengadilan	1392
Operasi domain saya gagal	1392
Operasi domain gagal karena informasi kontak yang tidak valid	1392
Gagal mentransfer domain saya ke Amazon Route 53	1393
Anda tidak mengeklik tautan di email otorisasi	1393
Kode otorisasi yang Anda dapatkan dari registrar saat ini tidak valid	1394

Kesalahan "Parameter dalam permintaan tidak valid" saat mencoba mentransfer domain .es ke Amazon Route 53	1394
Apakah nama domain internasional yang Anda transfer ke Amazon Route 53 terdaftar di punycode?	1394
Pesan kesalahan transfer umum	1395
Saya mengubah pengaturan DNS, tetapi mereka belum diterapkan	1397
Anda mentransfer layanan DNS ke Amazon Route 53 dalam 48 jam terakhir, sehingga DNS masih menggunakan layanan DNS Anda sebelumnya	1398
Anda baru saja mentransfer layanan DNS ke Amazon Route 53, tetapi Anda tidak memperbarui server nama dengan registrar domain	1398
DNS resolver masih menggunakan pengaturan lama untuk catatan	1400
Anda memiliki lebih dari satu zona yang di-hosting dengan nama yang sama, dan Anda memperbarui salah satu yang tidak terkait dengan domain	1400
Peramban saya menampilkan kesalahan "Server tidak ditemukan"	1402
Anda tidak membuat data untuk nama domain atau subdomain	1402
Anda membuat catatan, tetapi menentukan nilai yang salah	1403
Sumber daya tempat Anda mengarahkan lalu lintas tidak tersedia	1403
Saya tidak dapat merutekan lalu lintas ke bucket Amazon S3 yang dikonfigurasi untuk meng-host situs web	1403
Saya ditagih dua kali untuk zona yang di-hosting yang sama	1403
Saya ditagih beberapa faktur untuk domain saya	1404
AWS Akun saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53	1405
Rentang alamat IP	1406
Rentang alamat IP dari server nama Route 53	1406
Rentang alamat IP pemeriksaan kesehatan Route 53	1406
Mereferensikan daftar awalan	1407
Rentang alamat IP internal pemeriksaan kesehatan Route 53	1407
Memberikan tag ke sumber daya	1408
Tutorial	1410
Menggunakan Amazon Route 53 sebagai layanan DNS untuk subdomain tanpa memigrasi domain induk	1411
Membuat subdomain yang menggunakan Amazon Route 53 sebagai layanan DNS tanpa memigrasi domain induk	1412
Memigrasi layanan DNS untuk subdomain ke Amazon Route 53 tanpa memigrasi domain induk	1415

Transisi ke latensi berbasis perutean di Amazon Route 53	1419
Menambahkan Wilayah lain untuk perutean berbasis latensi Anda di Amazon Route 53	1422
Menggunakan latensi dan catatan tertimbang di Amazon Route 53 untuk merutekan lalu lintas ke EC2 beberapa instans Amazon di suatu Wilayah	1424
Mengelola lebih 100 catatan tertimbang di Amazon Route 53	1425
Menimbang jawaban multicatatan yang toleran terhadap kesalahan di Amazon Route 53	1426
Praktik terbaik	1429
Praktik terbaik untuk Amazon Route 53 DNS	1430
Praktik terbaik untuk VPC Resolver	1432
Hindari konfigurasi loop dengan titik akhir Resolver	1434
Penskalaan titik akhir penyelesai	1434
Ketersediaan tinggi untuk titik akhir Resolver	1436
Zona DNS berjalan	1436
Praktik terbaik untuk pemeriksaan kondisi Amazon Route 53	1436
Kuota	1439
Menggunakan Service Quotas untuk melihat dan mengelola kuota	1439
Kuota pada entitas	1439
Kuota pada domain	1440
Kuotas pada zona yang di-hosting	1440
Kuota pada catatan	1442
Kuota pada Route 53 VPC Resolver	1442
Kuota pada pemeriksaan kondisi	1449
Kuota pada konfigurasi log kueri	1450
Kuota tentang kebijakan alur lalu lintas dan catatan kebijakan	1450
Kuota pada set delegasi dapat digunakan kembali	1451
Kuota pada Profil Route 53	1451
Maksimum pada permintaan API	1452
Jumlah elemen dan karakter dalam permintaan ChangeResourceRecordSets	1452
Frekuensi permintaan API Amazon Route 53	1453
Frekuensi permintaan API Route 53 VPC Resolver	1453
Informasi terkait	1455
AWS sumber daya	1455
Alat dan pustaka pihak ketiga	1456
Antarmuka pengguna grafis	1457
Riwayat dokumen	1458
Rilis 2025	1458

Rilis 2024	1460
Rilis 2023	1462
Rilis 2022	1463
Rilis 2021	1464
Rilis 2020	1465
Rilis 2018	1465
Rilis 2017	1467
Rilis 2016	1469
Rilis 2015	1472
Rilis 2014	1475
Rilis 2013	1478
Rilis 2012	1480
Rilis 2011	1480
Rilis 2010	1480
.....	mcdlxxxi

Apa itu Amazon Route 53?

Amazon Route 53 adalah layanan web Domain Name System (DNS) yang dapat diskalakan dan sangat tersedia. Anda dapat menggunakan Route 53 untuk melakukan tiga fungsi utama dalam kombinasi apapun: pendaftaran domain, perutean DNS, dan pemeriksaan kondisi.

Jika Anda memilih untuk menggunakan Route 53 untuk ketiga fungsi tersebut, pastikan untuk mengikuti urutan di bawah ini:

1. Mendaftarkan nama domain

Situs web Anda memerlukan nama, seperti example.com. Route 53 memungkinkan Anda mendaftarkan nama untuk situs web atau aplikasi web Anda, yang dikenal sebagai nama domain.

- Untuk ikhtisar, lihat [Cara kerja pendaftaran domain](#).
- Untuk prosedur, lihat [Mendaftarkan domain baru](#).
- Untuk tutorial yang membawa Anda melalui pendaftaran domain dan membuat situs web sederhana dalam bucket Amazon S3, lihat [Memulai Amazon Route 53](#).

2. Rutekan lalu lintas internet ke sumber daya untuk domain Anda

Saat pengguna membuka peramban web dan memasukkan nama domain Anda (example.com) atau nama subdomain (acme.example.com) di bilah alamat, Route 53 membantu menghubungkan peramban dengan situs web atau aplikasi web Anda.

- Untuk ikhtisar, lihat [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#).
- Untuk prosedur, lihat [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#).
- Untuk prosedur tentang cara merutekan email ke Amazon WorkMail, lihat [Merutekan lalu lintas ke Amazon WorkMail](#).

3. Periksa kondisi sumber daya Anda

Route 53 mengirimkan permintaan otomatis melalui internet ke sumber daya, seperti server web, untuk memverifikasi bahwa itu dapat dijangkau, tersedia, dan berfungsi. Anda juga dapat memilih untuk menerima pemberitahuan ketika sumber daya menjadi tidak tersedia dan memilih untuk merutekan lalu lintas internet dari sumber daya dengan kondisi tidak baik.

- Untuk gambaran umum, lihat [Bagaimana Amazon Route 53 memeriksa kondisi sumber daya Anda](#).
- Untuk prosedur, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

Fitur Route 53 lainnya

Selain menjadi layanan web Domain Name System (DNS), Route 53 menawarkan fitur-fitur berikut:

VPC Resolver

Dapatkan DNS rekursif untuk Amazon Anda VPCs di Wilayah AWS, VPCs di AWS Outposts rak, atau jaringan lokal lainnya. Buat aturan penerusan bersyarat dan titik akhir Route 53 untuk menyelesaikan nama kustom yang dikuasai di zona host pribadi Route 53 atau di server DNS lokal Anda.

Untuk informasi lebih lanjut, lihat [Apa itu Route 53 VPC Resolver?](#).

Amazon Route 53 Resolver di Outposts

Hubungkan Resolver VPC di rak Outpost dengan server DNS di pusat data lokal Anda melalui titik akhir Resolver. Ini memungkinkan resolusi kueri DNS antara rak Outposts dan sumber daya lokal lainnya.

Untuk informasi lebih lanjut, lihat [Apa itu Amazon Route 53 di Outposts?](#).

Penyelesai DNS Firewall

Lindungi kueri DNS rekursif Anda dalam Resolver VPC. Buat daftar domain dan buat aturan firewall yang menyaring lalu lintas DNS keluar terhadap aturan ini.

Untuk informasi lebih lanjut, lihat [Menggunakan DNS Firewall untuk menyaring lalu lintas DNS keluar](#).

Arus Lalu Lintas

Easy-to-use dan manajemen lalu lintas global yang hemat biaya: mengarahkan pengguna akhir ke titik akhir terbaik untuk aplikasi Anda berdasarkan geoproximity, latensi, kesehatan, dan pertimbangan lainnya.

Untuk informasi lebih lanjut, lihat [Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS](#).

Profil Amazon Route 53

Dengan Route 53 Profiles, Anda dapat menerapkan dan mengelola konfigurasi Route 53 terkait DNS di banyak VPCs dan berbeda. Akun AWS

Untuk informasi lebih lanjut, lihat [Apa itu Profil Amazon Route 53?](#).

Topik

- [Cara kerja pendaftaran domain](#)
- [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#)
- [Bagaimana Amazon Route 53 memeriksa kondisi sumber daya Anda](#)
- [Konsep Amazon Route 53](#)
- [Cara memulai Amazon Route 53](#)
- [Mengakses Amazon Route 53](#)
- [AWS Identity and Access Management](#)
- [Harga dan penagihan Amazon Route 53](#)
- [Menggunakan Route 53 dengan AWS SDK](#)

Cara kerja pendaftaran domain

Jika Anda ingin membuat situs web atau aplikasi web, Anda mulai dengan mendaftarkan nama situs web Anda, yang dikenal sebagai [domain name](#). Nama domain Anda adalah nama, seperti example.com, yang dimasukkan pengguna di peramban untuk menampilkan situs web Anda.

Berikut ikhtisar cara mendaftarkan nama domain dengan Amazon Route 53:

1. Anda memilih nama domain dan mengonfirmasi bahwa itu tersedia, artinya tidak ada orang lain yang mendaftarkan nama domain yang Anda inginkan.

Jika nama domain yang Anda inginkan sudah digunakan, Anda dapat mencoba nama lain atau mencoba mengubah hanya domain tingkat atas, seperti .com, ke domain tingkat atas lainnya, seperti .ninja atau .hoki. Untuk daftar domain tingkat atas yang didukung Route 53, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

2. Anda mendaftar nama domain dengan Route 53. Saat Anda mendaftarkan domain, Anda memberikan nama dan informasi kontak untuk pemilik domain dan kontak lainnya.

Saat Anda mendaftarkan domain dengan Route 53, layanan secara otomatis membuat sendiri layanan DNS untuk domain dengan melakukan hal berikut:

- Membuat [hosted zone](#) yang memiliki nama yang sama dengan domain Anda.
- Menetapkan satu set empat server nama ke zona yang di-hosting. Saat seseorang menggunakan peramban untuk mengakses situs web Anda, seperti www.example.com, server nama ini memberi tahu peramban tempat untuk menemukan sumber daya Anda, seperti server

web atau bucket Amazon S3. ([Amazon S3](#) adalah penyimpanan objek untuk menyimpan dan mengambil sejumlah data dari mana pun di web. Bucket adalah kontainer untuk objek yang Anda simpan di S3.)

- Mendapat server nama dari zona host dan menambahkannya ke domain.

Untuk informasi selengkapnya, lihat [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#).

3. Di akhir proses pendaftaran, kami mengirimkan informasi Anda ke registrar untuk domain tersebut. [domain registrar](#) adalah baik Amazon Registrar, Inc. atau rekan registrar kami, Gandi. Untuk mengetahui siapa registrar untuk domain Anda, lihat [Menemukan registrar Anda](#).
4. Registrar mengirimkan informasi Anda ke Registri untuk domain. Registri adalah perusahaan yang menjual pendaftaran domain untuk satu atau beberapa domain tingkat atas, seperti .com.
5. Registri menyimpan informasi tentang domain Anda di basis data mereka sendiri dan juga menyimpan beberapa informasi di basis data WHOIS publik.

Untuk informasi selengkapnya tentang cara mendaftarkan nama domain, lihat [Mendaftarkan domain baru](#).

Jika Anda sudah mendaftarkan nama domain dengan registrar lain, Anda dapat memilih untuk mentransfer pendaftaran domain ke Route 53. Ini tidak diperlukan untuk menggunakan fitur Route 53 lainnya. Untuk informasi selengkapnya, lihat [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#).

Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda

Semua komputer di internet, dari ponsel pintar atau laptop Anda terhubung ke server yang melayani konten untuk situs web ritel besar, berkomunikasi satu sama lain dengan menggunakan angka. Angka-angka ini, dikenal sebagai Alamat IP, adalah salah satu dari format berikut:

- Format Internet Protocol versi 4 (IPv4), seperti 192.0.2.44
- Protokol Internet versi 6 (IPv6) format, seperti 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345

Saat Anda membuka peramban dan membuka situs web, Anda tidak perlu mengingat dan memasukkan string panjang karakter seperti itu. Sebagai gantinya, Anda dapat memasukkan nama

domain seperti example.com dan tetap berada di tempat yang tepat. Layanan DNS seperti Amazon Route 53 membantu membuat koneksi itu antara nama domain dan alamat IP.

Topik

- [Ikhtisar tentang cara Anda mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas internet untuk domain Anda](#)
- [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#)

Ikhtisar tentang cara Anda mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas internet untuk domain Anda

Berikut adalah ikhtisar tentang cara menggunakan konsol Amazon Route 53 untuk mendaftarkan nama domain dan mengonfigurasi Route 53 untuk merutekan lalu lintas internet ke situs web atau aplikasi web Anda.

1. Anda mendaftarkan nama domain yang Anda ingin pengguna Anda gunakan untuk mengakses konten Anda. Untuk gambaran umum, lihat [Cara kerja pendaftaran domain](#).
2. Setelah Anda mendaftarkan nama domain Anda, Route 53 secara otomatis membuat zona yang di-hosting publik yang memiliki nama yang sama dengan domain tersebut. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting publik](#).
3. Untuk merutekan lalu lintas ke sumber daya Anda, Anda membuat catatan, juga dikenal sebagai kumpulan catatan sumber daya, di zona yang di-hosting. Setiap catatan menyertakan informasi tentang bagaimana Anda ingin merutekan lalu lintas untuk domain Anda, seperti berikut ini:

Nama

Nama catatan sesuai dengan nama domain (example.com) atau nama subdomain (www.example.com, retail.example.com) yang Anda inginkan Route 53 untuk merutekan lalu lintas.

Nama setiap catatan di zona yang di-hosting harus diakhiri dengan nama zona yang di-hosting. Misalnya, jika nama zona yang di-hosting adalah example.com, semua nama catatan harus diakhiri dengan example.com. Konsol Route 53 melakukan ini untuk Anda secara otomatis.

Tipe

Jenis catatan biasanya menentukan jenis sumber daya yang Anda inginkan untuk dirutekan lalu lintas. Misalnya, untuk merutekan lalu lintas ke server email, Anda menentukan MX

untuk Type. Untuk merutekan lalu lintas ke server web yang memiliki alamat IPv4 IP, Anda menentukan A untuk Jenis.

Nilai

Nilai berkaitan erat dengan Tipe. Jika Anda menentukan MX untuk Tipe, Anda menentukan nama satu atau beberapa server email untuk Nilai. Jika Anda menentukan A untuk Jenis, Anda menentukan alamat IP dalam IPv4 format, seperti 192.0.2.136.

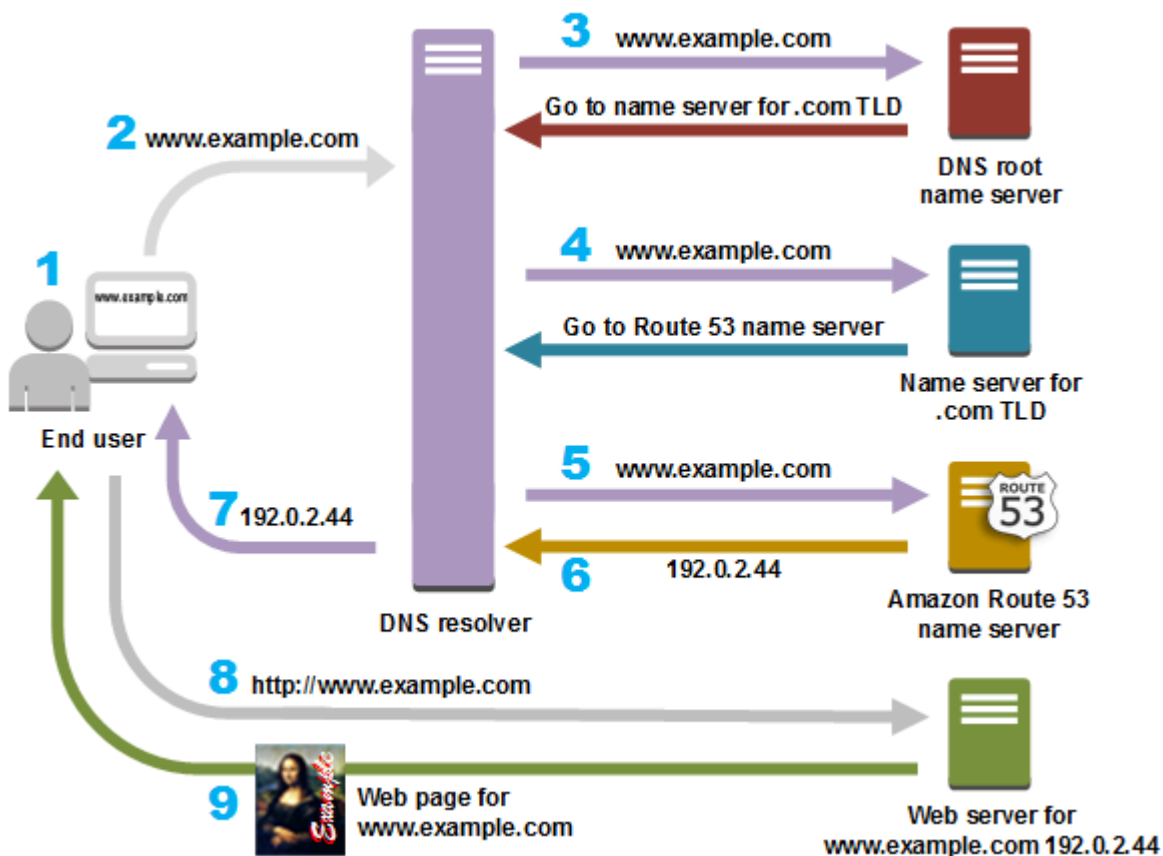
Untuk informasi lebih lanjut tentang catatan, lihat [Bekerja dengan catatan](#).

Anda juga dapat membuat catatan Route 53 khusus, yang disebut catatan alias, yang merutekan lalu lintas ke bucket Amazon S3, distribusi CloudFront Amazon, dan sumber daya lainnya. AWS Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#) dan [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Untuk informasi selengkapnya tentang perutean lalu lintas internet ke sumber daya Anda, lihat [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#).

Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda

Setelah Anda mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas internet Anda ke sumber daya Anda, seperti server web atau bucket Amazon S3, inilah yang terjadi hanya dalam beberapa milidetik ketika seseorang meminta konten untuk `www.example.com`:



1. Seorang pengguna membuka peramban web, memasukkan `www.example.com` di bilah alamat, dan menekan Enter.
2. Permintaan untuk `www.example.com` dirutekan ke DNS resolver, yang biasanya dikelola oleh penyedia layanan internet (ISP) pengguna, seperti penyedia internet kabel, penyedia broadband DSL, atau jaringan perusahaan.
3. DNS resolver untuk ISP meneruskan permintaan untuk `www.example.com` ke server nama root DNS.
4. DNS resolver meneruskan permintaan untuk `www.example.com` lagi, kali ini ke salah satu server nama TLD untuk domain `.com`. Server nama untuk domain `.com` merespons permintaan dengan nama keempat server nama Route 53 yang terkait dengan domain `example.com`.

DNS resolver men-cache (menyimpan) empat server nama Route 53. Saat berikutnya seseorang menjelajah ke `example.com`, resolver melewati langkah 3 dan 4 karena sudah memiliki server nama untuk `example.com`. Server nama biasanya di-cache selama dua hari.

5. DNS resolver memilih server nama Route 53 dan meneruskan permintaan untuk `www.example.com` ke server nama tersebut.

6. Server nama Route 53 terlihat di zona yang di-hosting example.com untuk catatan www.example.com, mendapatkan nilai terkait, seperti alamat IP untuk server web, 192.0.2.44, dan mengembalikan alamat IP ke DNS resolver.
7. DNS resolver akhirnya memiliki alamat IP yang dibutuhkan pengguna. Resolver menghasilkan nilai ke web peramban.

 Note

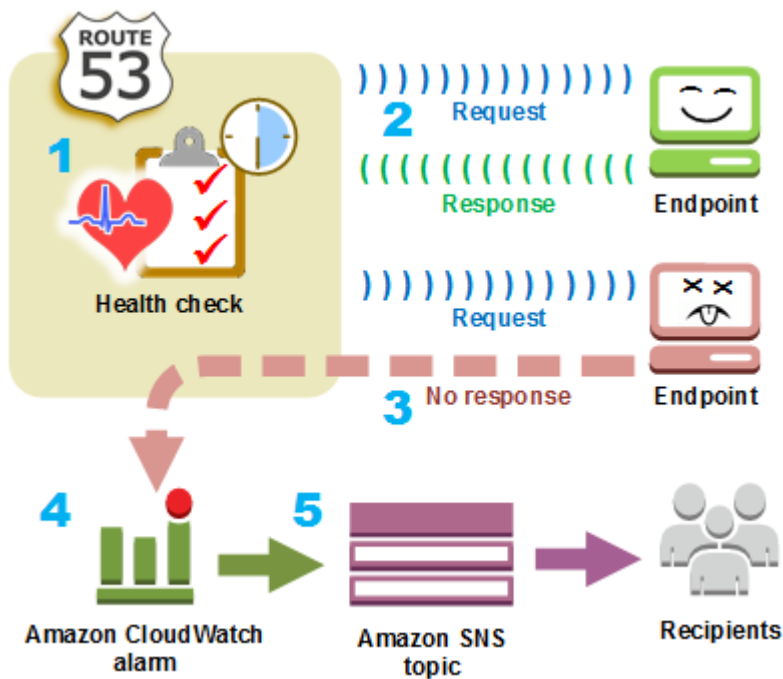
DNS resolver juga menyimpan alamat IP untuk example.com selama jangka waktu yang Anda tentukan sehingga dapat merespons lebih cepat saat berikutnya seseorang menelusuri example.com. Untuk informasi selengkapnya, lihat [time to live \(TTL\)](#).

8. Peramban web mengirimkan permintaan untuk www.example.com ke alamat IP yang didapatnya dari DNS resolver. Di sinilah konten Anda, misalnya, server web yang berjalan pada instans Amazon EC2 atau bucket Amazon S3 yang dikonfigurasi sebagai titik akhir situs web.
9. Server web atau sumber daya lain di 192.0.2.44 mengembalikan halaman web untuk www.example.com ke peramban web, dan peramban web menampilkan halaman tersebut.

Bagaimana Amazon Route 53 memeriksa kondisi sumber daya Anda

Pemeriksaan kondisi Amazon Route 53 memantau kondisi sumber daya Anda seperti server web dan server email. Anda dapat mengonfigurasi CloudWatch alarm Amazon secara opsional untuk pemeriksaan kesehatan, sehingga Anda menerima pemberitahuan saat sumber daya tidak tersedia.

Berikut adalah gambaran umum tentang cara kerja pemeriksaan kondisi jika Anda ingin diberi tahu saat sumber daya tidak tersedia:



1. Anda membuat pemeriksaan kondisi dan menentukan nilai yang menentukan cara kerja pemeriksaan kondisi, seperti berikut ini:

- Alamat IP atau nama domain titik akhir, seperti server web, yang Anda inginkan untuk dipantau oleh Route 53. (Anda juga dapat memantau status pemeriksaan kesehatan lainnya, atau keadaan CloudWatch alarm.)
- Protokol yang Anda ingin Amazon Route 53 gunakan untuk melakukan pemeriksaan: HTTP, HTTPS, atau TCP.
- Seberapa sering Anda ingin Route 53 mengirim permintaan ke titik akhir. Ini adalah interval permintaan.
- Berapa kali secara berturut-turut titik akhir harus gagal merespons permintaan sebelum Route 53 menganggapnya tidak sehat. Ini adalah ambang kegagalan.
- Secara opsional, bagaimana Anda ingin diberi tahu saat Route 53 mendeteksi bahwa titik akhir tidak sehat. Saat Anda mengonfigurasi notifikasi, Route 53 secara otomatis menyetel CloudWatch alarm. CloudWatch menggunakan Amazon SNS untuk memberi tahu pengguna bahwa titik akhir tidak sehat.

2. Route 53 mulai mengirim permintaan ke titik akhir pada interval yang Anda tentukan di pemeriksaan kondisi.

Jika titik akhir merespons permintaan, Route 53 menganggap titik akhir sehat dan tidak mengambil tindakan.

3. Jika titik akhir tidak menanggapi permintaan, Route 53 mulai menghitung jumlah permintaan berurutan yang tidak ditanggapi oleh titik akhir:
 - Jika hitungan mencapai nilai yang Anda tentukan untuk ambang kegagalan, Route 53 menganggap titik akhir tidak sehat.
 - Jika titik akhir mulai merespons lagi sebelum hitungan mencapai ambang kegagalan, Route 53 mengatur ulang hitungan ke 0, dan CloudWatch tidak menghubungi Anda.
4. Jika Route 53 menganggap titik akhir tidak sehat dan jika Anda mengonfigurasi pemberitahuan untuk pemeriksaan kesehatan, Route 53 memberi tahu CloudWatch.

Jika Anda tidak mengonfigurasi pemberitahuan, Anda masih dapat melihat status pemeriksaan kondisi Route 53 Anda di konsol Route 53. Untuk informasi selengkapnya, lihat [Memantau status pemeriksaan kondisi dan mendapatkan notifikasi](#).

5. Jika Anda mengonfigurasi pemberitahuan untuk pemeriksaan kesehatan, CloudWatch memicu alarm dan menggunakan Amazon SNS untuk mengirim pemberitahuan ke penerima yang ditentukan.

Selain memeriksa kondisi titik akhir yang ditentukan, Anda dapat mengonfigurasi pemeriksaan kondisi untuk memeriksa kondisi satu atau beberapa pemeriksaan kondisi lainnya sehingga Anda dapat diberi tahu ketika sejumlah sumber daya tertentu, seperti dua server web dari lima, tidak tersedia. Anda juga dapat mengonfigurasi pemeriksaan kesehatan untuk memeriksa status CloudWatch alarm sehingga Anda dapat diberi tahu berdasarkan berbagai kriteria, bukan hanya apakah sumber daya menanggapi permintaan.

Jika Anda memiliki beberapa sumber daya yang menjalankan fungsi yang sama, misalnya, server web atau server database, dan Anda ingin Route 53 merutekan lalu lintas hanya ke sumber daya yang sehat, Anda dapat mengonfigurasi failover DNS dengan mengaitkan pemeriksaan kesehatan dengan setiap catatan untuk sumber daya tersebut. Jika pemeriksaan kondisi menentukan bahwa sumber daya yang mendasarinya tidak sehat, Route 53 merutekan lalu lintas dari catatan terkait.

Untuk informasi selengkapnya tentang penggunaan Route 53 untuk memantau kondisi sumber daya Anda, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

Konsep Amazon Route 53

Berikut ini gambaran umum konsep yang dibahas di seluruh Panduan Developer Amazon Route 53.

Topik

- [Konsep pendaftaran domain](#)
- [Konsep Sistem Nama Domain \(Domain Name System/DNS\)](#)
- [Konsep bidang kontrol dan data](#)
- [Konsep pemeriksaan kondisi](#)

Konsep pendaftaran domain

Berikut gambaran umum tentang konsep-konsep yang terkait dengan pendaftaran domain.

- [domain name](#)
- [domain registrar](#)
- [domain registry](#)
- [domain reseller](#)
- [top-level domain \(TLD\)](#)

nama domain

Nama, seperti example.com, yang diketik pengguna di bilah alamat peramban web untuk mengakses situs web atau aplikasi web. Untuk membuat situs web atau aplikasi web Anda tersedia di internet, Anda mulai dengan mendaftarkan nama domain. Untuk informasi selengkapnya, lihat [Cara kerja pendaftaran domain](#).

registri domain

Perusahaan yang diakreditasi oleh ICANN (Internet Corporation for Assigned Names and Numbers) untuk memproses pendaftaran domain untuk domain tingkat atas tertentu (.). TLDs Untuk menemukan registrar domain Anda, lihat [Menemukan registrar Anda](#).

registri domain

Perusahaan yang memiliki hak untuk menjual domain yang memiliki domain tingkat atas tertentu. Misalnya, [VeriSign](#) adalah registri yang memiliki hak untuk menjual domain yang memiliki TLD .com. Registri domain menentukan aturan untuk mendaftarkan domain, seperti persyaratan tempat tinggal untuk TLD geografis. Registri domain juga memelihara basis data otoritatif untuk semua nama domain yang memiliki TLD yang sama. Basis data registri berisi informasi seperti informasi kontak dan server nama untuk setiap domain.

reseller domain

Perusahaan yang menjual nama domain untuk pendaftar seperti Amazon Registrar. Amazon Route 53 adalah reseller domain untuk Amazon Registrar dan untuk rekan registrar kami, Gandi.

domain tingkat atas (TLD)

Bagian terakhir dari nama domain, seperti .com, .org, atau .ninja. Ada dua tipe domain tingkat atas:

Domain tingkat atas umum

Ini TLDs biasanya memberi pengguna gambaran tentang apa yang akan mereka temukan di situs web. Misalnya, nama domain yang memiliki TLD .bike sering dikaitkan dengan situs web untuk bisnis atau organisasi sepeda motor atau sepeda. Dengan beberapa pengecualian, Anda dapat menggunakan TLD umum apa pun yang Anda inginkan, sehingga klub sepeda dapat menggunakan TLD .hockey untuk nama domain mereka.

Domain tingkat atas geografis

Ini TLDs terkait dengan wilayah geografis seperti negara atau kota. Beberapa pendaftar untuk geografis TLDs memiliki persyaratan residensi, sementara yang lain, seperti [the section called “.io \(Wilayah Samudra Hindia Britania\)”](#), mengizinkan atau bahkan mendorong penggunaan sebagai TLD generik.

Untuk daftar TLDs yang dapat Anda gunakan saat mendaftarkan nama domain dengan Route 53, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Konsep Sistem Nama Domain (Domain Name System/DNS)

Berikut adalah gambaran umum konsep yang berkaitan dengan Sistem Nama Domain (DNS).

- [alias record](#)
- [authoritative name server](#)
- [CIDR block](#)
- [DNS query](#)
- [DNS resolver](#)
- [Domain Name System \(DNS\)](#)
- [hosted zone](#)
- [IP address](#)

- [name servers](#)
- [private DNS](#)
- [recursive name server](#)
- [record \(DNS record\)](#)
- [reusable delegation set](#)
- [routing policy](#)
- [subdomain](#)
- [time to live \(TTL\)](#)

catatan alias

Jenis catatan yang dapat Anda buat dengan Amazon Route 53 untuk merutekan lalu lintas ke AWS sumber daya seperti CloudFront distribusi Amazon dan bucket Amazon S3. Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

server nama otoritatif

Server nama yang memiliki informasi definitif tentang satu bagian dari Sistem Nama Domain (DNS) dan yang merespons permintaan dari DNS resolver dengan mengembalikan informasi yang berlaku. Misalnya, server nama otoritatif untuk domain tingkat atas (TLD) .com mengetahui nama server nama untuk setiap domain .com yang terdaftar. Saat server nama .com otoritatif menerima permintaan dari DNS resolver untuk example.com, server tersebut merespons dengan nama server nama untuk layanan DNS untuk domain example.com.

Server nama Route 53 adalah server nama otoritatif untuk setiap domain yang menggunakan Route 53 sebagai layanan DNS. Server nama mengetahui bagaimana Anda ingin merutekan lalu lintas untuk domain dan subdomain Anda berdasarkan catatan yang Anda buat di zona yang di-hosting untuk domain tersebut. (Server nama Route 53 menyimpan zona yang di-hosting untuk domain yang menggunakan Route 53 sebagai layanan DNS.)

Misalnya, jika server nama Route 53 menerima permintaan untuk www.example.com, server akan menemukan catatan tersebut dan menghasilkan alamat IP, seperti 192.0.2.33, yang ditentukan dalam catatan.

Blok CIDR

Blok CIDR adalah rentang IP yang digunakan dengan perutean berbasis IP. Di Route 53 Anda dapat menentukan blok CIDR dari /0 hingga /24 untuk IPv4 dan /0 hingga /48 untuk IPv6. Misalnya, blok IPv4 CIDR /24 mencakup 256 alamat IP yang berdekatan. Anda dapat

mengelompokkan set blok CIDR (atau rentang IP) ke dalam lokasi CIDR, yang pada gilirannya dikelompokkan ke dalam koleksi CIDR yang dapat digunakan kembali.

Kueri DNS

Biasanya permintaan yang diajukan oleh perangkat, seperti komputer atau ponsel pintar, ke Sistem Nama Domain (DNS) untuk sumber daya yang terkait dengan nama domain. Contoh paling umum dari kueri DNS adalah ketika pengguna membuka peramban dan mengetikkan nama domain di bilah alamat. Respons terhadap permintaan DNS biasanya adalah alamat IP yang dikaitkan dengan sumber daya seperti server web. Perangkat yang memulai permintaan menggunakan alamat IP untuk berkomunikasi dengan sumber daya. Misalnya, peramban dapat menggunakan alamat IP untuk mendapatkan halaman web dari server web.

DNS resolver

Server DNS, sering kali dikelola oleh penyedia layanan internet (ISP), yang bertindak sebagai perantara antara permintaan pengguna dan server nama DNS. Saat Anda membuka peramban dan memasukkan nama domain di bilah alamat, kueri Anda akan terlebih dahulu masuk ke resolver DNS. Resolver berkomunikasi dengan server nama DNS untuk mendapatkan alamat IP untuk sumber daya yang sesuai, seperti server web. DNS resolver juga dikenal sebagai server nama rekursif karena mengirimkan permintaan ke urutan server nama DNS otoritatif hingga mendapat respons (biasanya alamat IP) yang dikembalikan ke perangkat pengguna, misalnya, peramban web di komputer laptop.

Sistem Nama Domain (DNS)

Jaringan server di seluruh dunia yang membantu komputer, ponsel pintar, tablet, dan perangkat berkemampuan IP lainnya untuk berkomunikasi satu sama lain. Sistem Nama Domain menerjemahkan nama yang mudah dipahami seperti `example.com` ke dalam angka, yang dikenal sebagai alamat IP, yang memungkinkan komputer untuk saling menemukan di internet.

Lihat juga [IP address](#).

Zona yang di-hosting

Kontainer untuk catatan, yang mencakup informasi tentang bagaimana Anda ingin merutekan lalu lintas untuk domain (seperti `example.com`) dan semua subdomainnya (seperti `www.example.com`, `retail.example.com`, dan `seattle.accounting.example.com`). Zona yang di-hosting memiliki nama yang sama dengan domain terkait.

Misalnya, zona yang di-hosting untuk `example.com` mungkin menyertakan catatan yang memiliki informasi tentang perutean lalu lintas untuk `www.example.com` ke server web yang memiliki

alamat IP 192.0.2.243, dan catatan yang memiliki informasi tentang perutean email misalnya .com ke dua server email, mail1.example.com dan mail2.example.com. Setiap server email juga membutuhkan catatan sendiri.

Lihat juga [record \(DNS record\)](#).

Alamat IP

Nomor yang ditetapkan ke perangkat di internet—seperti laptop, ponsel pintar, atau server web—yang memungkinkan perangkat berkomunikasi dengan perangkat lain di internet. Alamat IP dalam salah satu format berikut:

- Format Internet Protocol versi 4 (IPv4), seperti 192.0.2.44
- Protokol Internet versi 6 (IPv6) format, seperti 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345

Route 53 mendukung keduanya IPv4 dan IPv6 alamat untuk tujuan berikut:

- Anda dapat membuat catatan yang memiliki tipe A, untuk IPv4 alamat, atau jenis AAAA, untuk IPv6 alamat.
- Anda dapat membuat pemeriksaan kesehatan yang mengirim permintaan ke IPv4 atau ke IPv6 alamat.
- Jika resolver DNS berada di IPv6 jaringan, ia dapat menggunakan salah satu IPv4 atau IPv6 untuk mengirimkan permintaan ke Route 53.

server nama

Server di Domain Name System (DNS) yang membantu menerjemahkan nama domain ke alamat IP yang digunakan komputer untuk berkomunikasi satu sama lain. Server nama adalah server nama rekursif (juga dikenal sebagai [DNS resolver](#)) atau [authoritative name server](#).

Untuk gambaran umum tentang bagaimana DNS merutekan lalu lintas ke sumber daya Anda, termasuk peran Route 53 dalam prosesnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

DNS pribadi

Versi lokal Sistem Nama Domain (DNS) yang memungkinkan Anda merutekan lalu lintas untuk domain dan subdomainnya ke instans Amazon EC2 dalam satu atau beberapa awan pribadi virtual Amazon (). VPCs Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting privat](#).

catatan (catatan DNS)

Objek di zona yang di-hosting yang Anda gunakan untuk menentukan bagaimana Anda ingin merutekan lalu lintas untuk domain atau subdomain. Misalnya, Anda dapat membuat catatan untuk `example.com` dan `www.example.com` yang merutekan lalu lintas ke server web yang memiliki alamat IP `192.0.2.234`.

Untuk informasi lebih lanjut tentang catatan, termasuk informasi tentang fungsionalitas yang disediakan oleh catatan khusus Route 53, lihat [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#).

server nama rekursif

Lihat [DNS resolver](#).

rangkaian delegasi yang dapat digunakan kembali

Serangkaian yang terdiri dari empat server nama otoritatif yang dapat Anda gunakan dengan lebih dari satu zona yang di-hosting. Secara default, Route 53 memberikan pilihan acak server nama untuk setiap zona baru yang di-hosting. Untuk mempermudah migrasi layanan DNS ke Route 53 untuk domain dalam jumlah besar, Anda dapat membuat kumpulan delegasi yang dapat digunakan kembali, lalu mengaitkan kumpulan delegasi yang dapat digunakan kembali dengan zona baru yang di-hosting. (Anda tidak dapat mengubah server nama yang terkait dengan zona yang di-hosting yang ada.)

Anda membuat kumpulan delegasi yang dapat digunakan kembali dan mengaitkannya dengan zona yang di-hosting secara terprogram; menggunakan konsol Route 53 tidak didukung. Untuk informasi selengkapnya, lihat [CreateHostedZone](#) dan [CreateReusableDelegationSet](#) di Referensi API Amazon Route 53. Fitur yang sama juga tersedia di [AWS SDKs](#), [AWS Command Line Interface](#), dan [AWS Tools for Windows PowerShell](#).

kebijakan perutean

Pengaturan untuk rekaman yang menentukan bagaimana Route 53 merespons kueri DNS. Route 53 mendukung kebijakan perutean berikut:

- Kebijakan perutean sederhana – Gunakan untuk merutekan lalu lintas internet ke satu sumber daya yang menjalankan fungsi tertentu untuk domain Anda, misalnya, server web yang menyajikan konten untuk situs web `example.com`.
- Kebijakan perutean failover – Gunakan ketika Anda ingin mengonfigurasi failover aktif-pasif.
- Kebijakan perutean geolokasi – Gunakan saat Anda ingin merutekan lalu lintas internet ke sumber daya Anda berdasarkan lokasi pengguna Anda.

- Kebijakan perutean geoproximity – Gunakan saat Anda ingin merutekan lalu lintas berdasarkan lokasi sumber daya Anda dan, secara opsional, mengalihkan lalu lintas dari sumber daya di satu lokasi ke sumber daya di tempat lain.
- Kebijakan perutean latensi – Gunakan saat Anda memiliki sumber daya di beberapa lokasi dan Anda ingin merutekan lalu lintas ke sumber daya yang memberikan latensi terbaik.
- Kebijakan perutean berbasis IP — Gunakan saat Anda ingin merutekan lalu lintas berdasarkan lokasi pengguna Anda, dan dapatkan alamat IP tempat lalu lintas berasal.
- Kebijakan perutean jawaban multinilai – Gunakan saat Anda ingin Route 53 merespons kueri DNS dengan hingga delapan catatan sehat yang dipilih secara acak.
- Kebijakan perutean berbobot – Gunakan untuk merutekan lalu lintas ke beberapa sumber daya dalam proporsi yang Anda tentukan.

Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

subdomain

Nama domain yang memiliki satu atau lebih label yang ditambahkan ke nama domain terdaftar. Misalnya, jika Anda mendaftarkan nama domain `example.com`, maka `www.example.com` adalah subdomain. Jika Anda membuat `accounting.example.com` zona yang di-hosting untuk domain `example.com`, maka `seattle.accounting.example.com` adalah subdomain.

Untuk merutekan lalu lintas untuk subdomain, buat catatan yang memiliki nama yang Anda inginkan, seperti `www.example.com`, dan tentukan nilai yang berlaku, seperti alamat IP server web.

waktu untuk tayang (TTL)

Jumlah waktu, dalam detik, yang Anda inginkan DNS resolver untuk men-cache (menyimpan) nilai untuk catatan sebelum mengirimkan permintaan lain ke Route 53 untuk mendapatkan nilai saat ini untuk catatan itu. Jika DNS resolver menerima permintaan lain untuk domain yang sama sebelum TTL kedaluwarsa, resolver mengembalikan nilai yang di-cache.

TTL yang lebih lama mengurangi biaya Route 53 Anda, yang sebagian didasarkan pada jumlah kueri DNS yang ditanggapi oleh Route 53. TTL yang lebih pendek mengurangi jumlah waktu DNS resolver merutekan lalu lintas ke sumber daya yang lebih lama setelah Anda mengubah nilai dalam catatan, misalnya, dengan mengubah alamat IP untuk server web untuk `www.example.com`.

Konsep bidang kontrol dan data

Berikut ikhtisar konsep yang terkait dengan bagaimana Amazon Route 53 membagi fungsinya menjadi kontrol dan bidang data. Layanan Route 53 Layanan AWS, seperti kebanyakan, mencakup bidang kontrol yang memungkinkan Anda melakukan operasi manajemen seperti membuat, memperbarui, dan menghapus sumber daya, dan bidang data yang menyediakan fungsionalitas inti layanan. Sementara kedua fungsi dibangun agar dapat diandalkan, bidang kontrol dioptimalkan untuk konsistensi data, sedangkan bidang data dioptimalkan untuk ketersediaan. Desain tangguh pesawat data memungkinkannya untuk mempertahankan ketersediaan bahkan selama peristiwa mengganggu yang jarang terjadi, di mana pesawat kontrol mungkin menjadi tidak tersedia. Untuk alasan ini, kami merekomendasikan penggunaan fungsi bidang data di mana ketersediaan penting.

Untuk pemeriksaan DNS publik dan swasta Route 53 dan kesehatan, pesawat kontrol terletak di Wilayah AWS us-east-1 dan pesawat data didistribusikan secara global.

Amazon Route 53 dibagi menjadi bidang kontrol dan data sebagai berikut:

- Untuk DNS publik dan pribadi Route 53, pesawat kontrol terdiri dari Route 53 APIs, yang memungkinkan Anda untuk mengelola entri DNS, termasuk Route 53 dan Arus Lalu Lintas. APIs Konsol Route 53 terletak di Wilayah AWS us-east-1, tetapi AWS jika menentukan bahwa ada gangguan di Wilayah itu, konsol Route 53 akan dilayani oleh us-west-2. Wilayah AWS Pesawat data adalah layanan DNS otoritatif, yang berjalan di lebih dari 200 lokasi Points of Presence (PoP), menjawab kueri DNS berdasarkan zona host dan data pemeriksaan kesehatan Anda.
- Untuk pemeriksaan kesehatan Route 53, bidang kontrol terdiri dari Route 53 APIs yang dapat Anda gunakan untuk membuat, memperbarui, dan menghapus pemeriksaan kesehatan. Konsol pemeriksaan kesehatan Route 53 terletak di Wilayah AWS us-east-1, tetapi AWS jika menentukan bahwa ada gangguan di Wilayah itu, konsol pemeriksaan kesehatan Route 53 akan dilayani oleh us-west-2. Wilayah AWS Pesawat data adalah layanan yang didistribusikan secara global, yang melakukan pemeriksaan kesehatan, mengumpulkan hasil dan mengirimkannya ke pesawat data DNS publik dan swasta Route 53 dan. [AWS Global Accelerator](#)
- Untuk Resolver [VPC Route 53, bidang kontrol terdiri dari Resolver](#) VPC yang APIs memungkinkan Anda mengelola setelan VPC Amazon, aturan Resolver, kebijakan pencatatan kueri, dan kebijakan Firewall DNS. Bidang data adalah layanan penyelesaian DNS, yang menjawab kueri DNS di VPC Anda, titik akhir yang meneruskan kueri ke resolver lain, dan bidang data DNS Firewall yang menerapkan kebijakan untuk memfilter kueri DNS. VPC Resolver adalah layanan regional dan kontrol serta pesawat datanya berjalan secara independen di masing-masing. Wilayah AWS
- Pendaftaran domain Route 53 hanya dikelola pada pesawat kontrol di Wilayah AWS us-east-1.

Untuk informasi selengkapnya tentang bidang data, pesawat kontrol, dan cara AWS membangun layanan untuk memenuhi target ketersediaan tinggi, lihat [paper Stabilitas statis menggunakan Availability Zones](#) di Library Amazon Builders.

Konsep pemeriksaan kondisi

Berikut ini ikhtisar konsep yang terkait dengan pemeriksaan kondisi Amazon Route 53.

- [DNS failover](#)
- [endpoint](#)
- [health check](#)

failover DNS

Sebuah metode untuk merutekan lalu lintas dari sumber daya yang tidak sehat dan sumber daya yang sehat. Bila Anda memiliki lebih dari satu sumber daya yang menjalankan fungsi yang sama—misalnya, lebih dari satu server web atau server mail—Anda dapat mengonfigurasi pemeriksaan kesehatan Route 53 untuk memeriksa kesehatan sumber daya Anda dan mengonfigurasi catatan di zona yang dihosting untuk mengarahkan lalu lintas hanya ke sumber daya yang sehat.

Untuk informasi selengkapnya, lihat [Mengonfigurasi failover DNS](#).

titik akhir

Sumber daya, seperti server web atau server email, yang Anda konfigurasi pemeriksaan kondisi untuk memantau kondisinya. Anda dapat menentukan titik akhir berdasarkan IPv4 alamat (192.0.2.243), berdasarkan alamat (2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345), atau dengan IPv6 nama domain (example.com).

Note

Anda juga dapat membuat pemeriksaan kesehatan yang memantau status pemeriksaan kesehatan lainnya atau yang memantau keadaan alarm CloudWatch alarm.

pemeriksaan kesehatan

Komponen Route 53 yang memungkinkan Anda melakukan hal berikut:

- Pantau apakah titik akhir yang ditentukan, seperti server web, sehat

- Secara opsional, dapatkan pemberitahuan saat titik akhir menjadi tidak sehat
- Secara opsional, konfigurasi failover DNS, yang memungkinkan Anda untuk mengubah rute lalu lintas internet dari sumber daya yang tidak sehat ke sumber daya yang sehat

Untuk informasi selengkapnya tentang cara membuat dan menggunakan pemeriksaan kondisi, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

Cara memulai Amazon Route 53

Untuk informasi tentang memulai Amazon Route 53, lihat topik berikut dalam panduan ini:

- [Siapkan Amazon Route 53](#), yang menjelaskan cara mendaftar AWS, cara mengamankan akses ke AWS akun Anda, dan cara mengatur akses terprogram ke Route 53
- [Memulai Amazon Route 53](#), yang menjelaskan cara mendaftarkan nama domain, cara membuat bucket Amazon S3 dan mengonfigurasinya untuk meng-host situs web statis, dan cara merutekan lalu lintas internet ke situs web

Mengakses Amazon Route 53

Anda dapat mengakses Amazon Route 53 dengan cara berikut:

- Konsol Manajemen AWS— Prosedur di seluruh panduan ini menjelaskan cara menggunakan Konsol Manajemen AWS untuk melakukan tugas.
- AWS SDKsJika Anda menggunakan bahasa pemrograman yang AWS menyediakan SDK, Anda dapat menggunakan SDK untuk mengakses Route 53. SDKs menyederhanakan otentikasi, mengintegrasikan dengan mudah dengan lingkungan pengembangan Anda, dan menyediakan akses mudah ke perintah Route 53. Untuk informasi lebih lanjut, lihat [Alat untuk Amazon Web Services](#).
- API Route 53 – Jika Anda menggunakan bahasa pemrograman yang tidak tersedia untuk SDK, lihat [Referensi API Amazon Route 53](#) untuk informasi tentang tindakan API dan cara membuat permintaan API.
- AWS Command Line Interface – Untuk informasi selengkapnya, lihat [Menyiapkan AWS Command Line Interface](#) di Panduan Pengguna AWS Command Line Interface .
- AWS Tools for Windows PowerShell – Untuk informasi selengkapnya, lihat [Menyiapkan AWS Tools for Windows PowerShell](#) di AWS Tools for PowerShell Panduan Pengguna.

AWS Identity and Access Management

Amazon Route 53 terintegrasi dengan AWS Identity and Access Management (IAM), layanan yang memungkinkan organisasi Anda melakukan hal berikut:

- Buat pengguna dan grup di bawah AWS akun organisasi Anda
- Bagikan sumber daya AWS akun Anda dengan mudah di antara pengguna di akun
- Menetapkan kredensial keamanan unik untuk setiap pengguna
- Secara bertahap mengontrol akses pengguna ke layanan dan sumber daya

Misalnya, Anda dapat menggunakan IAM dengan Route 53 untuk mengontrol pengguna mana di AWS akun Anda yang dapat membuat zona host baru atau mengubah catatan.

Untuk informasi umum tentang IAM, lihat berikut ini:

- [Identity and access management di Amazon Route 53](#)
- [Identity and Access Management \(IAM\)](#)
- [Panduan Pengguna IAM](#)

Harga dan penagihan Amazon Route 53

Seperti AWS produk lainnya, tidak ada kontrak atau komitmen minimum untuk menggunakan Amazon Route 53. Anda hanya membayar untuk zona yang di-hosting yang Anda konfigurasi dan jumlah kueri DNS yang dijawab oleh Route 53. Untuk informasi lebih lanjut, lihat [Harga Amazon Route 53](#).

Untuk informasi tentang penagihan AWS layanan, termasuk cara melihat tagihan dan mengelola akun serta pembayaran, lihat [Panduan AWS Billing Pengguna](#).

Menggunakan Route 53 dengan AWS SDK

AWS kit pengembangan perangkat lunak (SDKs) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan developer untuk membangun aplikasi dalam bahasa pilihan mereka.

Dokumentasi SDK	Contoh kode
AWS SDK untuk C++	AWS SDK untuk C++ contoh kode
AWS CLI	AWS CLI contoh kode
AWS SDK for Go	AWS SDK for Go contoh kode
AWS SDK for Java	AWS SDK for Java contoh kode
AWS SDK untuk JavaScript	AWS SDK untuk JavaScript contoh kode
AWS SDK untuk Kotlin	AWS SDK untuk Kotlin contoh kode
AWS SDK for .NET	AWS SDK for .NET contoh kode
AWS SDK for PHP	AWS SDK for PHP contoh kode
AWS Tools for PowerShell	AWS Tools for PowerShell contoh kode
AWS SDK untuk Python (Boto3)	AWS SDK untuk Python (Boto3) contoh kode
AWS SDK for Ruby	AWS SDK for Ruby contoh kode
AWS SDK untuk Rust	AWS SDK untuk Rust contoh kode
AWS SDK untuk SAP ABAP	AWS SDK untuk SAP ABAP contoh kode
AWS SDK untuk Swift	AWS SDK untuk Swift contoh kode

Untuk contoh khusus untuk Route 53, lihat [Contoh kode untuk Route 53 menggunakan AWS SDKs](#).

 Ketersediaan contoh

Tidak dapat menemukan apa yang Anda butuhkan? Minta contoh kode menggunakan tautan Berikan umpan balik di bagian bawah halaman ini.

Memulai Amazon Route 53

Mulailah dengan langkah-langkah dasar dengan mendaftarkan domain dengan Amazon Route 53 dan mengonfigurasi Route 53 untuk menanggapi kueri DNS yang menyelesaikan ke situs web statis. Tutorial pertama menghosting situs web statis di bucket Amazon S3 terbuka, dan tutorial kedua menggunakan CloudFront distribusi Amazon untuk melayani situs web dengan SSL/TLS.

Perkiraan biaya

- Ada biaya tahunan untuk mendaftarkan domain, mulai dari 9 USD hingga beberapa ratus USD, tergantung pada domain tingkat atas, seperti .com. Untuk informasi selengkapnya, lihat [Harga Route 53 untuk Pendaftaran Domain](#). Biaya ini tidak dapat dikembalikan.
- Saat Anda mendaftarkan domain, kami secara otomatis membuat zona yang di-hosting dengan nama yang sama seperti domain. Anda menggunakan zona yang dihosting untuk menentukan di mana Anda ingin Route 53 untuk merutekan lalu lintas untuk domain Anda.
- Dalam tutorial ini, Anda membuat bucket Amazon S3 dan mengunggah halaman web sampel. Jika Anda adalah AWS pelanggan baru, Anda dapat memulai dengan Amazon S3 secara gratis. Jika Anda adalah AWS pelanggan lama, biaya didasarkan pada berapa banyak data yang Anda simpan, pada jumlah permintaan untuk data Anda, dan pada jumlah data yang ditransfer. Untuk informasi selengkapnya, lihat [Harga Amazon S3](#).
- CloudFront Biaya didasarkan pada jumlah permintaan untuk data Anda, jumlah lokasi edge yang Anda gunakan, dan jumlah data yang ditransfer. Untuk informasi selengkapnya, silakan lihat [Harga CloudFront](#).

Topik

- [Siapkan Amazon Route 53](#)
- [Gunakan domain Anda untuk situs web statis di bucket Amazon S3](#)
- [Gunakan CloudFront distribusi Amazon untuk melayani situs web statis](#)

Siapkan Amazon Route 53

Gambaran umum dan prosedur di bagian ini membantu Anda memulai AWS.

Topik

- [Mendaftar untuk Akun AWS](#)

- [Buat pengguna dengan akses administratif](#)
- [Unduh alat](#)

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirimkan Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [Konsol Manajemen AWS](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Unduh alat

Konsol Manajemen AWS Termasuk konsol untuk Amazon Route 53, tetapi jika Anda ingin mengakses layanan secara terprogram, lihat berikut ini:

- Panduan API mendokumentasikan operasi yang didukung layanan dan menyediakan tautan ke dokumentasi SDK dan CLI terkait:
 - [Referensi API Amazon Route 53](#)
- Untuk memanggil API tanpa harus menangani detail tingkat rendah seperti merakit permintaan HTTP mentah, Anda dapat menggunakan SDK. AWS SDKs Menyediakan fungsi dan tipe data yang merangkum fungsionalitas layanan. AWS Untuk mengunduh AWS SDK dan mengakses petunjuk penginstalan, lihat halaman yang berlaku:
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)
 - [Node.js](#)
 - [PHP](#)
 - [Python](#)
 - [Ruby](#)

Untuk daftar lengkapnya AWS SDKs, lihat [Alat untuk Amazon Web Services](#).

- Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk mengontrol beberapa AWS layanan dari baris perintah. Anda juga dapat mengotomatiskan perintah Anda menggunakan skrip. Untuk informasi selengkapnya, lihat [AWS Command Line Interface](#).
- AWS Tools for Windows PowerShell mendukung AWS layanan ini. Untuk informasi selengkapnya, lihat [AWS Tools for PowerShell Referensi Cmdlet](#).

Gunakan domain Anda untuk situs web statis di bucket Amazon S3

Tutorial ini menunjukkan cara menggunakan Amazon Route 53 untuk merutekan lalu lintas DNS untuk domain Anda ke bucket Amazon Simple Storage Service yang menghosting situs web statis. Anda akan membuat catatan alias yang mengarahkan domain Anda ke titik akhir situs web S3.

Tutorial ini adalah bagian dari alur kerja penyiapan situs web statis lengkap. Untuk informasi umum tentang merutekan lalu lintas ke bucket S3 apa pun, lihat. [Merutekan lalu lintas ke situs web yang di-host di bucket Amazon S3](#)

Setelah selesai, pengunjung dapat mengakses situs web statis Anda menggunakan nama domain khusus Anda.

Note

Anda juga dapat mentransfer domain yang ada ke Route 53, tetapi prosesnya lebih kompleks dan memakan waktu daripada mendaftarkan domain baru. Untuk informasi selengkapnya, lihat [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#).

Prasyarat

Sebelum Anda mulai, selesaikan langkah-langkah ini:

- Selesaikan langkah-langkah dalam [Siapkan Amazon Route 53](#).
- Daftarkan nama domain menggunakan Amazon Route 53. Untuk informasi selengkapnya, lihat [Mendaftarkan domain baru](#).
- Konfigurasi bucket Amazon Simple Storage Service untuk hosting situs web statis. Untuk petunjuk selengkapnya, lihat [Tutorial: Mengonfigurasi situs web statis menggunakan domain kustom yang terdaftar dengan Route 53](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Saat Anda menyelesaikan tutorial Amazon Simple Storage Service, Anda akan memiliki:

- Bucket Amazon S3 dikonfigurasi untuk hosting dan pengalihan situs web (jika menggunakan subdomain www)
- Konten situs web diunggah ke bucket Anda
- Akses publik dikonfigurasi untuk bucket situs web Anda

Langkah 1: Rutekan lalu lintas DNS untuk domain Anda ke bucket situs web Anda

Sekarang setelah Anda memiliki bucket Amazon Simple Storage Service yang dikonfigurasi untuk hosting situs web statis, gunakan Amazon Route 53 untuk merutekan lalu lintas DNS untuk domain Anda ke bucket. Ini memungkinkan pengunjung untuk mengakses situs web Anda menggunakan nama domain khusus Anda.

Cara merutekan lalu lintas ke situs web

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.

Note

Ketika Anda mendaftarkan domain, Amazon Route 53 secara otomatis membuat zona yang di-hosting dengan nama yang sama. Zona yang dihosting berisi informasi tentang bagaimana Anda ingin Route 53 merutekan lalu lintas untuk domain.

3. Dalam daftar zona yang di-hosting, pilih nama domain Anda.
4. Pilih Create record (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Nama catatan

Biarkan kosong untuk membuat catatan untuk domain root Anda.

Tipe catatan

Pilih A - Rute lalu lintas ke IPv4 alamat dan beberapa AWS sumber daya.

Alias

Nyalakan Alias.

Rute lalu lintas ke

Pilih titik akhir situs web Alias ke S3.

Pilih Wilayah tempat Anda membuat bucket S3.

Pilih ember S3 Anda. Nama bucket harus sesuai dengan nama domain Anda. Dalam daftar, nama bucket muncul dengan titik akhir situs web Amazon S3 untuk Wilayah tempat bucket dibuat, misalnya, `s3-website-us-west-1.amazonaws.com` (`example.com`)

Jika bucket Anda tidak muncul dalam daftar, masukkan titik akhir situs web Amazon S3 untuk Wilayah tempat bucket dibuat, misalnya, **`s3-website-us-west-2.amazonaws.com`**

Untuk daftar lengkap titik akhir situs web Amazon S3, lihat [Titik akhir Situs Web Amazon S3](#).

Mengevaluasi Kondisi Target

Terima nilai default Tidak.

6. Pilih Create records (Buat catatan).

(Opsional) Cara menambahkan catatan alias untuk subdomain Anda (**www.example.com**)

Jika Anda membuat bucket untuk subdomain, tambahkan catatan alias untuk domain itu juga.

1. Pilih Create record (Buat catatan).
2. Tentukan nilai-nilai berikut ini:

Nama catatan

Masukkan **www**.

Tipe catatan

Pilih A - Rute lalu lintas ke IPv4 alamat dan beberapa AWS sumber daya.

Alias

Nyalakan Alias.

Rute lalu lintas ke

Pilih titik akhir situs web Alias ke S3.

Pilih Wilayah tempat Anda membuat bucket S3.

Pilih bucket S3 Anda untuk subdomain, misalnya, `s3-website-us-west-2.amazonaws.com` (**www.example.com**)

Mengevaluasi Kondisi Target

Terima nilai default Tidak.

3. Pilih Create records (Buat catatan).

Langkah 2: Uji situs web Anda

Untuk memverifikasi bahwa situs web berfungsi dengan benar, buka browser web dan telusuri ke yang berikut URLs:

- `http://your-domain-name`, misalnya, `example.com` - Menampilkan dokumen indeks dalam ember `your-domain-name`
- `http://www.your-domain-name` misalnya, `www.example.com` — Mengalihkan permintaan Anda ke bucket `your-domain-name`

di beberapa kasus, Anda mungkin perlu membersihkan cache untuk melihat perilaku yang diharapkan.

Untuk informasi lanjutan tentang perutean lalu lintas internet, lihat [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#). Untuk informasi tentang merutekan lalu lintas internet Anda ke AWS sumber daya, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Note

Amazon S3 tidak mendukung akses HTTPS ke situs web. Jika Anda ingin menggunakan HTTPS, Anda dapat menggunakan Amazon CloudFront untuk melayani situs web statis yang dihosting di Amazon S3. Untuk informasi selengkapnya, lihat [Gunakan CloudFront distribusi Amazon untuk melayani situs web statis](#).

Gunakan CloudFront distribusi Amazon untuk melayani situs web statis

Tutorial ini menunjukkan cara menggunakan Amazon Route 53 untuk merutekan lalu lintas DNS untuk domain Anda ke CloudFront distribusi Amazon yang melayani situs web statis. Anda akan membuat catatan alias yang mengarahkan domain dan subdomain Anda ke CloudFront distribusi.

Tutorial ini adalah bagian dari alur kerja penyiapan situs web statis lengkap. Untuk informasi umum tentang merutekan lalu lintas ke CloudFront distribusi apa pun, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#).

Setelah selesai, pengunjung dapat mengakses situs web Anda menggunakan nama domain khusus Anda dengan keamanan HTTPS yang disediakan oleh CloudFront.

Prasyarat

Sebelum Anda mulai, selesaikan langkah-langkah ini:

- Selesaikan langkah-langkah dalam [Siapkan Amazon Route 53](#).
- Daftarkan nama domain menggunakan Amazon Route 53. Untuk informasi selengkapnya, lihat [Mendaftarkan domain baru](#).
- Buat situs web statis yang aman menggunakan Amazon CloudFront dan Amazon Simple Storage Service. Untuk petunjuk selengkapnya, lihat [Memulai situs web statis aman](#) di Panduan CloudFront Pengembang Amazon.

Saat Anda menyelesaikan CloudFront tutorial Amazon, Anda akan memiliki:

- SSL/TLS Sertifikat untuk domain Anda di AWS Certificate Manager
- Bucket Amazon S3 dikonfigurasi untuk hosting dan pengalihan situs web
- CloudFront distribusi untuk domain root dan subdomain Anda

Langkah 1: Rutekan lalu lintas DNS untuk domain Anda ke distribusi Anda CloudFront

Sekarang setelah Anda memiliki CloudFront distribusi Amazon untuk situs web Anda, gunakan Amazon Route 53 untuk merutekan lalu lintas DNS untuk domain Anda ke distribusi. Ini memungkinkan pengunjung untuk mengakses situs web Anda menggunakan nama domain khusus Anda.

Untuk informasi selengkapnya tentang merutekan lalu lintas ke CloudFront distribusi, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#)

Cara merutekan lalu lintas ke situs web

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.

Note

Ketika Anda mendaftarkan domain, Amazon Route 53 secara otomatis membuat zona yang di-hosting dengan nama yang sama. Zona yang dihosting berisi informasi tentang bagaimana Anda ingin Route 53 merutekan lalu lintas untuk domain.

3. Dalam daftar zona yang di-hosting, pilih nama domain Anda.

4. Pilih **Create record** (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Nama catatan

Untuk catatan subdomain Anda, masukkan **www**.

Tipe catatan

Pilih **A - Rute lalu lintas ke IPv4 alamat dan beberapa AWS sumber daya**.

Alias

Nyalakan **Alias**.

Rute lalu lintas ke

Pilih **Alias** untuk CloudFront didistribusikan.

Pilih Wilayah **us-east-1**.

Pilih CloudFront distribusi Anda. Nama distribusi harus cocok dengan nama yang muncul di kolom Nama domain di CloudFront konsol, misalnya, `dddjjjkkk.cloudfront.net`.

Mengevaluasi Kondisi Target

Terima nilai default **Tidak**.

6. Pilih **Create records** (Buat catatan).

Untuk menambahkan rekaman alias untuk domain root Anda (**example.com**)

Tambahkan catatan alias untuk domain root Anda juga, sehingga mengarah ke CloudFront distribusi yang mengarahkan lalu lintas ke. `www.example.com`

1. Pilih **Create record** (Buat catatan).
2. Tentukan nilai-nilai berikut ini:

Nama catatan

Biarkan kosong untuk membuat catatan untuk domain root Anda.

Tipe catatan

Pilih **A - Rute lalu lintas ke IPv4 alamat dan beberapa AWS sumber daya**.

Alias

Nyalakan Alias.

Rute lalu lintas ke

Pilih Alias untuk CloudFront didistribusikan.

Pilih Wilayah us-east-1.

Pilih CloudFront distribusi domain root Anda.

Mengevaluasi Kondisi Target

Terima nilai default Tidak.

3. Pilih Create records (Buat catatan).

Langkah 2: Uji situs web Anda

Untuk memverifikasi bahwa situs web berfungsi dengan benar, buka browser web dan telusuri ke yang berikut URLs:

- `https://www.your-domain-name`, misalnya, `www.example.com` — Menampilkan dokumen indeks dalam `www.your-domain-name` ember
- `https://your-domain-name`misalnya, `example.com` — Mengalihkan permintaan Anda ke bucket `www.your-domain-name`

di beberapa kasus, Anda mungkin perlu membersihkan cache untuk melihat perilaku yang diharapkan.

Untuk informasi lanjutan tentang perutean lalu lintas internet, lihat [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#). Untuk informasi tentang merutekan lalu lintas internet Anda ke AWS sumber daya, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Mengintegrasikan dengan layanan lain

Anda dapat mengintegrasikan Amazon Route 53 dengan AWS layanan lain untuk mencatat permintaan yang dikirim ke API Route 53, memantau status sumber daya, dan menetapkan tag ke sumber daya Anda. Selain itu, Anda dapat menggunakan Route 53 untuk merutekan lalu lintas internet ke AWS sumber daya Anda.

Topik

- [Pencatatan, pemantauan, dan penandaan](#)
- [Merutekan lalu lintas ke sumber daya lain AWS](#)

Pencatatan, pemantauan, dan penandaan

AWS CloudTrail

Amazon Route 53 terintegrasi dengan AWS CloudTrail, layanan yang menangkap informasi tentang setiap permintaan yang dikirim ke API Route 53 oleh AWS akun Anda. Anda dapat menggunakan informasi dalam file CloudTrail log untuk menentukan permintaan mana yang dibuat ke Route 53, alamat IP sumber dari mana setiap permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan sebagainya.

Untuk informasi selengkapnya, lihat [Mencatat panggilan API Amazon Route 53 dengan AWS CloudTrail](#).

Amazon CloudWatch

Anda dapat menggunakan Amazon CloudWatch untuk memantau status — sehat atau tidak sehat — dari pemeriksaan kesehatan Route 53 Anda. Pemeriksaan kondisi memantau kondisi dan performa aplikasi web, server web, dan sumber daya lainnya. Pada interval reguler yang Anda tentukan, Route 53 mengirimkan permintaan otomatis melalui internet ke aplikasi, server, atau sumber daya lain untuk memverifikasi bahwa semuanya dapat dijangkau, tersedia, dan fungsional.

Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

Editor Tag

Tag adalah label yang Anda tetapkan ke AWS sumber daya, termasuk domain Route 53, zona yang dihosting, dan pemeriksaan kesehatan. Setiap tanda memiliki sebuah kunci dan sebuah nilai, yang keduanya ditentukan oleh Anda. Misalnya, Anda mungkin menetapkan tanda ke pendaftaran domain yang memiliki kunci "Customer" dan nilai "Example Corp." Anda dapat menggunakan tag untuk berbagai tujuan; satu penggunaan umum adalah untuk mengkategorikan dan melacak biaya Anda AWS .

Untuk informasi selengkapnya, lihat [Memberi tanda pada sumber daya Amazon Route 53](#).

Merutekan lalu lintas ke sumber daya lain AWS

Anda dapat menggunakan Amazon Route 53 untuk merutekan lalu lintas ke berbagai AWS sumber daya.

Amazon API Gateway

Amazon API Gateway memungkinkan Anda membuat, menerbitkan, memelihara, memantau, dan mengamankan APIs pada skala apa pun. Anda dapat membuat akses APIs itu AWS atau layanan web lainnya, serta data yang disimpan di AWS Cloud.

Anda dapat menggunakan Route 53 untuk merutekan lalu lintas ke API Gateway API. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke API Amazon API Gateway dengan menggunakan nama domain Anda](#).

Amazon CloudFront

Untuk mempercepat pengiriman konten web Anda, Anda dapat menggunakan Amazon CloudFront, jaringan pengiriman AWS konten (CDN). CloudFront dapat mengirimkan seluruh situs web Anda — termasuk konten dinamis, statis, streaming, dan interaktif — dengan menggunakan jaringan global lokasi tepi. CloudFront merutekan permintaan konten Anda ke lokasi tepi yang memberi pengguna latensi terendah. Anda dapat menggunakan Route 53 untuk merutekan lalu lintas domain Anda ke CloudFront distribusi Anda. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#).

Amazon EC2

Amazon EC2 menyediakan kapasitas komputasi yang dapat diskalakan di AWS Cloud. Anda dapat meluncurkan lingkungan komputasi EC2 virtual (instance) menggunakan templat yang telah

dikonfigurasi sebelumnya (Amazon Machine Image, atau AMI). Ketika Anda meluncurkan EC2 instans, EC2 secara otomatis menginstal sistem operasi (Linux atau Microsoft Windows) dan perangkat lunak tambahan yang disertakan dalam AMI, seperti server web atau perangkat lunak database.

Jika Anda meng-host situs web atau menjalankan aplikasi web pada sebuah EC2 instance, Anda dapat merutekan lalu lintas untuk domain Anda, seperti `example.com`, ke server Anda dengan menggunakan Route 53. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke instans Amazon EC2](#).

AWS Elastic Beanstalk

Jika Anda menggunakan AWS Elastic Beanstalk untuk menyebarkan dan mengelola aplikasi di AWS Cloud, Anda dapat menggunakan Route 53 untuk merutekan lalu lintas DNS untuk domain Anda, seperti `example.com`, ke lingkungan Elastic Beanstalk. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke lingkungan AWS Elastic Beanstalk](#).

Penyeimbang Beban Elastis

Jika Anda meng-host situs web di beberapa EC2 instans Amazon, Anda dapat mendistribusikan lalu lintas ke situs web Anda di seluruh instans dengan menggunakan penyeimbang beban Elastic Load Balancing (ELB). Layanan ELB secara otomatis menskalakan penyeimbang beban saat lalu lintas ke situs web berubah seiring waktu. Penyeimbang beban juga memantau kondisi target yang terdaftar dan merutekan lalu lintas domain hanya ke target yang sehat.

Anda dapat menggunakan Route 53 untuk merutekan lalu lintas domain Anda ke Classic, Application, atau Network Load Balancer Anda. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke penyeimbang beban ELB](#).

Amazon Lightsail

Amazon Lightsail menyediakan kapasitas dan kemampuan komputasi, penyimpanan, serta jaringan untuk men-deploy juga mengelola situs web, aplikasi web, dan basis data di cloud dengan harga bulanan yang rendah serta dapat diprediksi.

Jika Anda menggunakan Lightsail, Anda dapat menggunakan Route 53 untuk merutekan lalu lintas ke instance Lightsail Anda. Untuk informasi selengkapnya, lihat [Menggunakan Route 53 untuk mengarahkan domain ke instans Amazon Lightsail](#).

Amazon S3

Amazon Simple Storage Service (Amazon S3), menyediakan penyimpanan cloud yang aman, tahan lama, dan sangat dapat diskalakan. Anda dapat mengonfigurasi bucket S3 untuk meng-host

situs web statis yang dapat mencakup halaman web dan skrip sisi klien. (S3 tidak mendukung pembuatan skrip sisi server.) Anda dapat menggunakan Route 53 untuk merutekan lalu lintas ke bucket Amazon S3. Untuk informasi selengkapnya, lihat topik berikut:

- Untuk informasi tentang perutean lalu lintas ke bucket, lihat [Merutekan lalu lintas ke situs web yang di-host di bucket Amazon S3](#).
- Untuk penjelasan yang lebih detail tentang cara meng-host situs web statis dalam bucket S3, lihat [Memulai Amazon Route 53](#).

Amazon Virtual Private Cloud (Amazon VPC)

Endpoint antarmuka memungkinkan Anda terhubung ke layanan yang didukung oleh AWS PrivateLink. Layanan ini mencakup beberapa AWS layanan, layanan yang diselenggarakan oleh AWS pelanggan lain dan mitra mereka sendiri VPCs (disebut sebagai layanan titik akhir), dan layanan AWS Marketplace mitra yang didukung.

Anda dapat menggunakan Route 53 untuk merutekan lalu lintas ke titik akhir antarmuka. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke titik akhir antarmuka Amazon Virtual Private Cloud dengan menggunakan nama domain Anda](#).

Amazon WorkMail

Jika Anda menggunakan Amazon WorkMail untuk email bisnis Anda dan Anda menggunakan Route 53 sebagai layanan DNS Anda, Anda dapat menggunakan Route 53 untuk merutekan lalu lintas ke domain WorkMail email Amazon Anda. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke Amazon WorkMail](#).

Untuk mengetahui informasi selengkapnya, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Format nama domain DNS

Nama domain (termasuk nama domain, zona yang di-hosting, dan catatan) terdiri dari serangkaian label yang dipisahkan oleh titik. Setiap label dapat berukuran hingga 63 byte. Panjang total nama domain tidak dapat melebihi 255 byte, termasuk titik. Amazon Route 53 mendukung nama domain yang valid.

Persyaratan penamaan tergantung pada apakah Anda mendaftarkan nama domain atau Anda menentukan nama zona yang di-hosting atau catatan. Lihat topik yang sesuai.

Memformat nama domain untuk pendaftaran nama domain

Untuk pendaftaran, nama domain hanya dapat berisi karakter a-z, 0-9, dan - (tanda hubung). Anda tidak dapat meletakkan tanda hubung di awal atau akhir label.

Untuk informasi tentang cara mendaftarkan nama domain internasionalisasi (IDN), lihat [Memformat nama domain yang diinternasionalisasi](#).

Memformat nama domain untuk zona yang di-hosting dan catatan

Untuk zona yang di-hosting dan catatan, nama domain dapat mencakup salah satu karakter ASCII yang dapat dicetak berikut (tidak termasuk spasi):

- a-z
- 0-9
- - (tanda hubung)
- ! " # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } ~ .

Amazon Route 53 menyimpan karakter abjad sebagai huruf kecil (a-z), terlepas dari cara Anda menentukannya: sebagai huruf besar, huruf kecil, atau huruf yang sesuai dalam kode escape.

Jika nama domain Anda berisi salah satu karakter berikut, Anda harus menentukan karakter dengan menggunakan kode escape dalam format *three-digit octal code*:

- Karakter 000 hingga 040 oktal (0 hingga 32 desimal, 0x00 hingga 0x20 heksadesimal)
- Karakter 177 hingga 377 oktal (127 hingga 255 desimal, 0x7F hingga 0xFF heksadesimal)

- . (titik), karakter 056 oktal (46 desimal, 0x2E heksadesimal), jika digunakan sebagai karakter dalam nama domain. Saat menggunakan . sebagai pembatas antara label, Anda tidak perlu menggunakan kode escape.

Jika nama domain menyertakan karakter selain a hingga z, 0 hingga 9, - (tanda hubung), atau _ (garis bawah), tindakan API Route 53 mengembalikan karakter sebagai kode escape. Ini yang terjadi jika Anda menentukan karakter sebagai karakter atau kode escape saat membuat entitas. Konsol Route 53 menampilkan karakter sebagai karakter, bukan sebagai kode escape.

Untuk daftar karakter ASCII kode oktal yang sesuai, lakukan pencarian internet tentang "tabel ascii".

Untuk menentukan nama domain yang diinternasionalisasi (IDN), ubah namanya menjadi Punycode. Untuk informasi selengkapnya, lihat [Memformat nama domain yang diinternasionalisasi](#).

Menggunakan tanda bintang (*) dalam nama zona yang di-hosting dan catatan

Anda dapat membuat zona yang di-hosting dan catatan yang menyertakan * dalam namanya.

Zona yang dihosting

- Anda tidak dapat menyertakan * di label paling kiri dalam nama domain. Misalnya, *.example.com tidak diperbolehkan.
- Jika Anda menyertakan * di posisi mana pun, DNS akan memperlakukannya sebagai karakter * (ASCII 42), bukan sebagai wildcard.

Rekaman

DNS memperlakukan karakter * sebagai wildcard atau sebagai karakter * (ASCII 42), tergantung di mana karakter muncul dalam nama. Perhatikan pembatasan berikut tentang penggunaan * sebagai wildcard pada nama catatan:

- Tanda * harus mengganti label paling kiri dalam nama domain, misalnya, *.example.com atau *.acme.example.com. Jika Anda menyertakan * di posisi lain, seperti prod*.example.com, DNS akan memperlakukannya sebagai karakter * (ASCII 42), bukan sebagai wildcard.
- Tanda * harus mengganti seluruh label. Misalnya, Anda tidak dapat menentukan *prod.example.com atau prod*.example.com.

- Nama domain tertentu akan diutamakan. Misalnya, jika Anda membuat catatan untuk *.example.com dan acme.example.com, Route 53 akan selalu merespons kueri DNS untuk acme.example.com dengan nilai dalam catatan acme.example.com.
- Tanda * diterapkan ke kueri DNS untuk tingkat subdomain yang menyertakan tanda bintang, dan semua subdomain dari subdomain tersebut. Misalnya, jika Anda membuat rekaman bernama *.example.com, Route 53 menggunakan nilai dalam rekaman tersebut untuk menanggapi kueri DNS untuk zenith.example.com, acme.zenith.example.com, dan pinnacle.acme.zenith.example.com (jika tidak ada catatan jenis apa pun untuk zona yang dihosting tersebut).

Jika Anda membuat catatan bernama *.example.com dan tidak ada catatan example.com, Route 53 akan merespons kueri DNS untuk example.com dengan NXDOMAIN (domain yang tidak ada).

Note

Jika Anda menggunakan Route 53 dengan AWS Certificate Manager, perhatikan bahwa sertifikat wildcard ACM hanya melindungi satu level subdomain. Misalnya, sertifikat ACM untuk *.example.com melindungi login.example.com dan test.example.com, tetapi tidak test.login.example.com. Untuk informasi selengkapnya, lihat [karakteristik dan batasan AWS Certificate Manager sertifikat](#).

- Anda dapat mengonfigurasi Route 53 agar mengembalikan respons yang sama untuk kueri DNS, baik untuk semua subdomain di tingkat yang sama dan untuk nama domain. Misalnya, Anda dapat mengonfigurasi Route 53 untuk merespons kueri DNS seperti acme.example.com dan zenith.example.com menggunakan catatan example.com. Lakukan langkah-langkah berikut ini:
 1. Buat catatan untuk domain, seperti example.com.
 2. Buat catatan alias untuk subdomain, seperti *.example.com. Tentukan catatan yang Anda buat di langkah 1 sebagai target untuk catatan alias.
- Anda tidak dapat menggunakan * sebagai wildcard untuk catatan yang memiliki tipe NS.

Memformat nama domain yang diinternasionalisasi

Ketika mendaftarkan nama domain baru atau membuat zona yang di-hosting dan catatan, Anda dapat menentukan huruf selain a-z (misalnya, ç dalam bahasa Prancis), karakter dalam huruf lain (misalnya, Sirilik atau Arab), dan karakter dalam bahasa Cina, Jepang, atau Korea. Amazon Route

53 menyimpan nama domain internasional ini (IDNs) di Punycode, yang mewakili karakter Unicode sebagai string ASCII.

Jika Anda mendaftarkan nama domain, perhatikan hal berikut:

- Anda dapat menggunakan karakter selain a-z, 0-9, dan - (tanda hubung) hanya jika domain tingkat atas (TLD) mendukung IDNs dan mendukung bahasa yang ingin Anda gunakan. Untuk menentukan bahasa yang didukung TLD, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).
- Anda dapat menentukan nama dalam bahasa yang tidak didukung jika nama hanya berisi huruf a-z. Misalnya, jika TLD tidak mendukung bahasa Prancis tetapi nama yang ingin Anda gunakan hanya menyertakan karakter a-z tanpa tanda diakritik, Anda tetap dapat menggunakan nama itu. Dalam contoh ini, nama yang menyertakan "c" diperbolehkan; nama yang berisi "ç" tidak diperbolehkan.
- Jika TLD tidak mendukung IDNs atau tidak mendukung bahasa yang ingin Anda gunakan untuk nama domain Anda, Anda juga tidak dapat menentukan nama di Punycode meskipun Punycode hanya menyertakan a-z, 0-9, dan -.

Contoh berikut menunjukkan representasi Punycode dari nama domain yang diinternasionalisasi 中国.asia:

```
xn--fiqs8s.asia
```

Saat Anda memasukkan IDN di bilah alamat peramban modern, peramban mengubahnya menjadi Punycode sebelum mengirimkan kueri DNS atau membuat permintaan HTTP.

Cara memasukkan IDN tergantung pada apa yang Anda buat (nama domain, zona yang di-hosting, atau catatan), dan bagaimana Anda membuatnya (API, SDK, atau konsol Route 53):

- Jika Anda menggunakan API Route 53 atau salah satunya AWS SDKs, Anda dapat mengonversi nilai Unicode secara terprogram ke Punycode. Misalnya, jika menggunakan Java, Anda dapat mengubah nilai Unicode ke Punycode menggunakan metode `toASCII` pada pustaka `java.net.IDN`.
- Jika menggunakan konsol Route 53 untuk mendaftarkan nama domain, Anda dapat menempelkan nama, termasuk karakter Unicode, ke bidang nama, dan konsol mengubah nilai ke Punycode sebelum menyimpannya.
- Jika menggunakan konsol Route 53 untuk membuat zona yang di-hosting atau catatan, Anda harus mengubah nama domain menjadi Punycode sebelum memasukkan nama dalam bidang

Nama yang sesuai. Untuk informasi tentang pengubah online, lakukan pencarian internet di "punycode converter".

Jika Anda mendaftarkan nama domain, perhatikan bahwa tidak semua domain tingkat atas (TLDs) mendukung IDNs. Untuk daftar yang TLDs didukung oleh Route 53, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#). TLDs yang tidak mendukung IDNs dicatat.

Mendaftarkan dan mengelola domain menggunakan Amazon Route 53

Ketika Anda ingin mendapatkan nama domain baru, seperti example.com bagian dari URL `http://example.com`, Anda dapat mendaftarkannya dengan Amazon Route 53. Anda juga dapat mentransfer pendaftaran untuk domain yang ada dari registrar lain ke Route 53 atau mentransfer pendaftaran untuk domain yang Anda daftarkan dengan Route 53 ke registrar lain.

Prosedur dalam bab ini menjelaskan cara mendaftarkan dan mentransfer domain menggunakan konsol Route 53, dan cara mengedit pengaturan domain dan melihat status domain. Jika Anda hanya mendaftar dan mengelola beberapa domain, menggunakan konsol adalah cara termudah.

Jika Anda perlu mendaftar dan mengelola banyak domain, Anda mungkin lebih suka membuat perubahan secara terprogram. Untuk informasi selengkapnya, lihat [Siapkan Amazon Route 53](#).

Note

Jika Anda menggunakan bahasa yang memiliki AWS SDK, gunakan SDK daripada mencoba untuk menyelesaikannya. APIs SDKs Membuat otentikasi lebih sederhana, mengintegrasikan dengan mudah dengan lingkungan pengembangan Anda, dan menyediakan akses mudah ke perintah Route 53.

Layanan pendaftaran nama domain disediakan berdasarkan [Perjanjian Pendaftaran Nama Domain](#).

Topik

- [Mendaftarkan domain baru](#)
- [Memperbarui pengaturan domain](#)
- [Memperbarui pendaftaran untuk domain](#)
- [Memulihkan domain yang kedaluwarsa atau dihapus](#)
- [Mengganti zona yang di-hosting untuk domain yang terdaftar di Route 53](#)
- [Mentransfer domain](#)
- [Mengirim ulang email otorisasi dan konfirmasi](#)
- [Mengonfigurasi DNSSEC untuk domain](#)

- [Menemukan registrar Anda dan informasi lain tentang domain Anda](#)
- [Menghapus pendaftaran nama domain](#)
- [Menghubungi AWS Support tentang masalah pendaftaran domain](#)
- [Mengunduh laporan penagihan domain](#)
- [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Mendaftarkan domain baru

Bagian ini mencakup topik-topik berikut yang terkait dengan pendaftaran domain baru dengan Amazon Route 53:

1. [Mendaftarkan domain baru](#):

- Pelajari step-by-step prosedur untuk mendaftar domain baru menggunakan konsol Route 53.
- Memahami pertimbangan dan prasyarat untuk pendaftaran domain, seperti menghubungi AWS Support untuk masalah, penetapan harga, domain tingkat atas yang didukung (TLDs), dan pembuatan zona host otomatis.

2. [Nilai yang Anda tentukan saat mendaftar atau mentransfer domain](#):

- Temukan nilai yang perlu Anda berikan saat mendaftar atau mentransfer domain, termasuk informasi kontak, pengaturan perlindungan privasi, dan opsi perpanjangan otomatis.
- Memahami implikasi dari perubahan nilai tertentu, seperti pemilik domain atau alamat email pendaftar.

3. [Nilai yang dikembalikan Amazon Route 53 saat Anda mendaftar domain](#):

- Pelajari tentang nilai yang dikembalikan Route 53 setelah pendaftaran domain berhasil, termasuk tanggal pendaftaran, tanggal kedaluwarsa, kode status domain, status kunci transfer, dan server nama.

4. [Melihat status pendaftaran domain](#):

- Cari tahu cara melihat status pendaftaran domain Anda saat ini, termasuk kode status ICANN dan tindakan apa pun yang diperlukan dari pihak Anda, seperti memverifikasi alamat email pendaftar.

Mendaftarkan domain baru

Daftarkan domain baru atau perbarui server nama untuk domain yang ada

Anda dapat menggunakan Amazon Route 53 dengan domain yang Anda daftarkan dengan Route 53, dan dengan domain yang telah Anda daftarkan dengan penyedia DNS lainnya. Tergantung pada penyedia DNS Anda, pilih salah satu prosedur berikut untuk mendaftar dan menggunakan domain baru dengan Route 53:

- Untuk mendaftarkan domain baru, lihat [Untuk mendaftarkan domain baru menggunakan Route 53](#).
- Untuk domain yang sudah ada, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).
- Untuk memindahkan domain ke registrar lain, lihat [memperbarui server nama saat Anda ingin menggunakan layanan DNS lain](#).

Pertimbangan untuk pendaftaran domain

Sebelum Anda mulai, perhatikan hal berikut:

Menghubungi AWS Support

Jika Anda mengalami masalah saat mendaftarkan domain, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Harga pendaftaran domain

Untuk informasi tentang biaya pendaftaran domain, lihat [Harga Amazon Route 53 untuk Pendaftaran Domain](#).

Domain yang didukung

Untuk daftar yang didukung TLDs, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Anda tidak dapat mengubah nama domain setelah Anda mendaftarkannya

Jika Anda tidak sengaja mendaftarkan nama domain yang salah, Anda tidak dapat mengubahnya. Sebagai gantinya, Anda perlu mendaftarkan nama domain lain dan menentukan nama yang benar. Anda juga tidak bisa mendapatkan pengembalian dana untuk nama domain yang Anda daftarkan secara tidak sengaja.

AWS kredit

Anda tidak dapat menggunakan AWS kredit untuk membayar biaya pendaftaran domain baru dengan Route 53.

Harga khusus atau premium

Registri TLD telah menetapkan harga khusus atau premium untuk beberapa nama domain. Anda tidak dapat menggunakan Route 53 untuk mendaftarkan domain yang memiliki harga khusus atau premium.

Biaya untuk zona yang di-hosting

Saat Anda mendaftarkan domain dengan Route 53, kami secara otomatis membuat zona yang di-hosting untuk domain tersebut dan membebankan sedikit biaya bulanan untuk zona yang di-hosting selain biaya tahunan untuk pendaftaran domain. Zona yang dihosting ini adalah tempat Anda menyimpan informasi tentang cara merutekan lalu lintas untuk domain Anda, misalnya, ke instans Amazon EC2 atau distribusi. CloudFront Jika Anda tidak ingin menggunakan domain Anda sekarang, Anda dapat menghapus zona yang di-hosting; jika Anda menghapusnya dalam waktu 12 jam setelah mendaftarkan domain, tidak akan ada biaya untuk zona yang di-hosting pada tagihan AWS Anda. Kami juga membebankan sedikit biaya untuk kueri DNS yang kami terima untuk domain Anda. Untuk informasi lebih lanjut, lihat [Harga Amazon Route 53](#).

Mengganti zona yang di-hosting untuk domain

Jika Anda membuat zona host baru untuk domain, Anda juga harus memperbarui server nama agar domain tersebut menggunakan server nama yang sama dengan zona host baru. Untuk detailnya, lihat [Mengganti zona yang di-hosting untuk domain yang terdaftar di Route 53](#)

Untuk mendaftarkan domain baru menggunakan Route 53

Untuk mendaftarkan domain baru menggunakan Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain dan kemudian Domain terdaftar.
3. Pada halaman Domain terdaftar, pilih Daftarkan domain.
 - a. Di bagian Cari domain, masukkan nama domain yang ingin Anda daftarkan, dan pilih Cari untuk mengetahui apakah nama domain tersebut tersedia.

Jika nama domain yang ingin Anda daftarkan berisi karakter selain a-z, A-Z, 0-9, dan - (tanda hubung), perhatikan hal-hal berikut:

- Anda dapat memasukkan nama menggunakan karakter yang berlaku. Anda tidak perlu mengonversi nama menjadi Punycode.
- Daftar bahasa akan muncul. Pilih bahasa dari nama yang ditentukan. Misalnya, jika Anda memasukkan příklad ("contoh" dalam bahasa Ceko), pilih Ceko (CES) atau Ceko (CZE).

 Note

Untuk bahasa yang memiliki lebih dari satu kode, Anda mungkin perlu mencoba keduanya. Meskipun CES dan CZE sama, beberapa registri TLD hanya mendukung satu atau yang lain.

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

Jika domain yang Anda masukkan tersedia, itu akan ditampilkan, jika tidak, domain serupa akan ditampilkan sebagai saran.

Anda dapat memilih hingga lima domain untuk mendaftar. Domain yang Anda pilih muncul di daftar Domain yang dipilih.

- Untuk mendaftarkan lebih banyak domain, ulangi langkah 3a hingga 3b.
- Pilih Lanjutkan ke checkout.
 - Pada halaman Harga, pilih jumlah tahun yang Anda inginkan untuk mendaftarkan domain dan apakah Anda ingin kami memperbarui pendaftaran domain Anda secara otomatis sebelum tanggal kedaluwarsa.

 Note

Pendaftaran dan perpanjangan nama domain tidak bisa mendapatkan pengembalian dana. Jika Anda mengaktifkan perpanjangan domain otomatis dan Anda memutuskan bahwa Anda tidak menginginkan nama domain setelah kami memperbarui pendaftaran, Anda tidak bisa mendapatkan pengembalian dana untuk biaya perpanjangan.

Pilih Berikutnya.

6. Pada halaman Informasi kontak, masukkan informasi kontak untuk pendaftar domain, admin, teknologi, dan kontak penagihan. Nilai yang Anda masukkan di sini diterapkan ke semua domain yang Anda daftarkan. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat mendaftar atau mentransfer domain](#).

 Important

Kontak yang Anda daftarkan sebagai pendaftar selama pendaftaran domain akan memiliki hak tertentu sebagai Pemegang Nama Terdaftar dari nama domain, di bawah Kebijakan [Transfer ICANN](#). Sebagian besar domain akan dihapus setelah penutupan Anda Akun AWS (untuk informasi lebih lanjut, lihat [AWS Akun saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53](#)), namun jika domain tetap berada di akun tertutup, kontak yang Anda daftarkan sebagai pendaftar mungkin memiliki kemampuan untuk meminta transfer nama domain ke pencatat eksternal. Oleh karena itu, kontak pendaftar yang Anda cantumkan sebaiknya adalah diri Anda sendiri atau orang lain yang Anda percayai untuk bertindak secara bertanggung jawab.

Perhatikan pertimbangan berikut:

Nama Depan dan Nama Belakang

Untuk Nama Depan dan Nama Belakang, kami sarankan Anda mencantumkan nama tersebut pada ID resmi Anda. Untuk beberapa perubahan pada pengaturan domain, beberapa registri domain mengharuskan Anda memberikan bukti identitas. Nama di ID Anda harus sesuai dengan nama kontak pendaftar untuk domain tersebut.

Kontak yang berbeda

Secara default, kami menggunakan informasi yang sama untuk ketiga kontak tersebut. Jika Anda ingin memasukkan informasi yang berbeda untuk satu atau beberapa kontak, ubah nilai Sama seperti kontak pendaftar sakelar sakelar ke posisi mati.

 Note

Untuk domain .it, pendaftar dan kontak administratif harus sama.

 Note

Untuk domain.jp, kontak teknis dan administratif harus sama.

Beberapa domain

Jika Anda mendaftarkan lebih dari satu domain, kami menggunakan informasi kontak yang sama untuk semua domain.

Informasi tambahan yang diperlukan

Untuk beberapa domain tingkat atas (TLDs), kami diminta untuk mengumpulkan informasi tambahan. Untuk ini TLDs, masukkan nilai yang berlaku setelah bidang Kode Postal/Pos.

Perlindungan privasi

Pilih apakah Anda ingin menyembunyikan informasi kontak Anda dari kueri WHOIS.

 Note

Anda harus menentukan pengaturan privasi yang sama untuk kontak administratif, pendaftar, teknis, dan penagihan.

Untuk informasi selengkapnya, lihat topik berikut:

- [Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain](#)
- [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

 Note

Untuk mengaktifkan perlindungan privasi untuk domain.uk, .co.uk, .me.uk, dan .org.uk, Anda harus membuka kasus dukungan dan meminta perlindungan privasi.

Pilih Berikutnya.

7. Pada halaman Ulasan, tinjau informasi yang Anda masukkan, dan perbaiki secara opsional, baca persyaratan layanan, dan pilih kotak centang untuk mengonfirmasi bahwa Anda telah membaca persyaratan layanan.

Pilih Kirim.

8. Di panel navigasi, pilih Domain dan kemudian Permintaan.

Pada halaman ini Anda dapat melihat status domain dan juga jika Anda perlu menanggapi email verifikasi kontak pendaftar. Anda juga dapat memilih untuk mengirim ulang email verifikasi.

Jika Anda menentukan alamat email untuk kontak pendaftar yang belum pernah digunakan untuk mendaftarkan domain dengan Route 53, beberapa pendaftar TLD mengharuskan Anda memverifikasi bahwa alamat tersebut valid.

Kami mengirim email verifikasi dari salah satu alamat email berikut:

- `noreply@registrar.amazon` - untuk TLDs didaftarkan oleh Amazon Registrar.
- `noreply@domainnameverification.net` atau `noreply@emailverification.info` — untuk TLDs didaftarkan oleh rekanan registrar kami, Gandi. Untuk menentukan registrar TLD Anda, lihat [Menemukan registrar Anda](#).

 Important

Kontak pendaftar harus mengikuti petunjuk dalam email untuk memverifikasi bahwa email telah diterima, atau kami harus menangguhkan domain seperti yang disyaratkan oleh ICANN. Jika ditangguhkan, domain tersebut tidak dapat diakses di internet.

- a. Saat Anda menerima email verifikasi, pilih tautan di email yang memverifikasi bahwa alamat email tersebut valid. Jika Anda tidak segera menerima email tersebut, periksa folder email sampah Anda.
 - b. Kembali ke halaman Permintaan. Jika status tidak diperbarui secara otomatis untuk mengatakan alamat email diverifikasi, segarkan browser.
9. Setelah pendaftaran domain selesai, langkah Anda selanjutnya tergantung apakah Anda ingin menggunakan Route 53 atau layanan DNS lain sebagai layanan DNS untuk domain tersebut:

- Route 53 — Di zona host yang dibuat Route 53 saat Anda mendaftarkan domain, buat catatan untuk memberi tahu Route 53 bagaimana Anda ingin merutekan lalu lintas untuk domain dan subdomain.

Misalnya, ketika seseorang memasukkan nama domain Anda di peramban dan kueri itu diteruskan ke Route 53, apakah Anda ingin Route 53 merespons kueri dengan alamat IP server web di pusat data Anda atau dengan nama penyeimbang beban ELB?

Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).

 Important

Jika Anda membuat rekaman di zona yang di-hosting selain yang dibuat oleh Route 53 secara otomatis, Anda harus memperbarui server nama domain untuk menggunakan server nama untuk zona baru yang di-hosting.

- Layanan DNS lainnya – Konfigurasi domain baru Anda untuk merutekan kueri DNS ke layanan DNS lainnya. Lakukan prosedur [Memperbarui server nama untuk menggunakan registrar lain](#).

Nilai yang Anda tentukan saat mendaftar atau mentransfer domain

 Note

Kami telah memperbarui konsol domain untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama, atau menggunakan konsol baru. Sebagian besar informasi yang dikembalikan oleh Route 53 adalah sama untuk kedua konsol. Perbedaannya dicatat dalam daftar berikut.

Saat Anda mendaftarkan domain atau mentransfer pendaftaran domain ke Amazon Route 53, Anda menentukan nilai yang dijelaskan dalam topik ini.

 Note

Jika Anda mendaftarkan lebih dari satu domain, Route 53 menggunakan nilai yang Anda tentukan untuk semua domain yang ada di keranjang belanja Anda.

Anda juga dapat mengubah nilai untuk domain yang saat ini terdaftar di Route 53. Perhatikan hal-hal berikut:

- Jika Anda mengubah informasi kontak untuk domain, kami mengirimkan email pemberitahuan ke kontak pendaftar tentang perubahan tersebut. Email ini berasal dari noreply@registrar.amazon. Untuk sebagian besar perubahan, kontak pendaftar tidak perlu merespons.
- Untuk perubahan informasi kontak yang juga merupakan perubahan kepemilikan, kami mengirimkan email tambahan kepada kontak pendaftar. ICANN mengharuskan kontak pendaftar mengonfirmasi penerimaan email. Untuk informasi selengkapnya, lihat Nama Depan, Nama Belakang dan Organisasi, nanti di bagian ini.

Untuk informasi selengkapnya tentang mengubah setelan untuk domain yang ada, lihat [Memperbarui pengaturan domain](#).

Nilai yang Anda tentukan

- [My Registrant, Administrative, and Technical contacts are all the same](#)
- [Contact Type](#)
- [First Name, Last Name](#)
- [Organization](#)
- [Email](#)
- [Phone](#)
- [Address 1](#)
- [Address 2](#)
- [Country](#)
- [State](#)
- [City](#)
- [Postal/Zip Code](#)
- [Fields for selected top-level domains](#)
- [Privacy Protection](#)
- [Auto-renew](#)

Sama seperti kontak pendaftar

Menentukan apakah Anda ingin menggunakan informasi kontak yang sama untuk pendaftar domain, kontak administratif, dan kontak teknis.

Jenis Kontak

Kategori untuk kontak ini. Perhatikan hal-hal berikut:

- Jika Anda memilih opsi selain Orang, Anda harus memasukkan nama organisasi.
- Bagi sebagian orang TLDs, perlindungan privasi yang tersedia tergantung pada nilai yang Anda pilih untuk Jenis Kontak. Untuk pengaturan perlindungan privasi untuk TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).
- Untuk domain .es, nilai Jenis Kontak harus Orang untuk ketiga kontak.

Nama Depan, Nama Belakang

Nama pertama dan terakhir dari kontak.

Important

Untuk Nama Depan dan Nama Belakang, kami sarankan Anda mencantumkan nama tersebut pada ID resmi Anda. Untuk beberapa perubahan pada pengaturan domain, Anda harus memberikan bukti identitas, dan nama pada ID Anda harus sesuai dengan nama kontak pendaftar untuk domain tersebut.

Jika Anda mentransfer domain ke Route 53 dan berikut ini benar, berarti Anda mengubah pemilik domain:

- Jenis kontak adalah Orang.
- Anda mengubah bidang Nama Belakang and/or Nama Depan untuk kontak pendaftar dari pengaturan saat ini.

Dalam hal ini, ICANN mengharuskan kami mengirim email ke kontak pendaftar untuk mendapatkan persetujuan. Kami mengirim email dari salah satu alamat email berikut:

TLDs	Alamat email tempat asal email persetujuan atau konfirmasi
TLDs terdaftar oleh Amazon Registrar	noreply@registrar.amazon

TLDs	Alamat email tempat asal email persetujuan atau konfirmasi
.fr	nic@nic.fr (Email dikirim ke kontak pendaftar saat ini dan kontak pendaftar baru.)
Semua yang lain	noreply@domainnameverification.net atau noreply@emailverification.info

Untuk menentukan registrar TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Important

Kontak pendaftar harus mengikuti petunjuk dalam email untuk mengonfirmasi bahwa email telah diterima, atau kami harus menangguhkan domain seperti yang disyaratkan oleh ICANN. Jika ditangguhkan, domain tersebut tidak dapat diakses di internet.

Jika Anda mengubah alamat email kontak pendaftar, email ini dikirim ke alamat email sebelumnya dan alamat email baru untuk kontak pendaftar.

Beberapa registrar TLD mengenakan biaya untuk mengubah pemilik domain. Saat Anda mengubah salah satu nilai ini, konsol Route 53 menampilkan pesan yang memberi tahu Anda apakah ada biaya.

Organisasi

Organisasi yang terkait dengan kontak, jika ada. Untuk kontak pendaftar dan administratif, ini biasanya adalah organisasi yang mendaftarkan domain. Untuk kontak teknis, ini mungkin organisasi yang mengelola domain.

Bila jenis kontak adalah nilai apa pun kecuali Orang dan Anda mengubah bidang Organisasi untuk kontak pendaftar, Anda mengubah pemilik domain. ICANN mengharuskan kami mengirim email ke kontak pendaftar untuk mendapatkan persetujuan. Kami mengirim email dari salah satu alamat email berikut:

TLDs	Alamat email tempat asal email persetujuan atau konfirmasi
TLDs terdaftar oleh Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (Email dikirim ke kontak pendaftar saat ini dan kontak pendaftar baru.)
Semua yang lain	noreply@domainnameverification.net atau noreply@emailverification.info

Untuk menentukan registrar TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Jika Anda mengubah alamat email kontak pendaftar, email ini dikirim ke alamat email sebelumnya dan alamat email baru untuk kontak pendaftar.

Beberapa registrar TLD mengenakan biaya untuk mengubah pemilik domain. Saat Anda mengubah nilai Organisasi, konsol Route 53 menampilkan pesan yang memberi tahu Anda apakah ada biaya.

Email

Alamat email untuk kontak.

Jika Anda mengubah alamat email untuk kontak pendaftar, kami mengirimkan email pemberitahuan ke alamat email sebelumnya dan alamat email baru. Email ini berasal dari noreply@registrar.amazon.

Telepon

Nomor telepon untuk kontak:

- Jika Anda memasukkan nomor telepon untuk lokasi di Amerika Serikat atau Kanada, masukkan 1 di kolom pertama dan 10-digit kode area dan nomor telepon di kolom kedua.
- Jika Anda memasukkan nomor telepon untuk lokasi lain, masukkan kode negara di bidang pertama, dan masukkan nomor telepon lainnya di bidang kedua. Untuk daftar kode negara telepon, lihat artikel Wikipedia [Daftar kode panggilan negara](#).

Alamat 1

Alamat jalan untuk kontak.

Alamat 2

Informasi alamat tambahan untuk kontak, misalnya, nomor apartemen atau perhentian surat.

Negara

Negara untuk kontak.

Negara

Negara bagian atau provinsi untuk kontak, jika ada.

Kota

Kota untuk kontak.

Kode Pos

Kode pos untuk kontak.

Bidang untuk domain tingkat atas yang dipilih

Domain tingkat atas berikut (TLDs) mengharuskan Anda menentukan nilai tambahan:

- .com.au dan .net.au
- .ca
- .es
- .fi
- .fr
- .it
- .ru
- .se
- .sg
- .co.uk, .me.uk, .org.uk, dan .uk

Selain itu, banyak yang TLDs memerlukan nomor identifikasi PPN.

Untuk informasi tentang nilai yang valid, lihat [ExtraParam](#) di Referensi API Amazon Route 53.

Perlindungan Privasi

Apakah Anda ingin menyembunyikan informasi kontak Anda dari kueri WHOIS. Jika Anda memilih Aktifkan perlindungan privasi (konsol baru) atau Sembunyikan informasi kontak (konsol lama), pertanyaan WHOIS (“siapa”) akan mengembalikan informasi kontak untuk pencatat atau nilai “Dilindungi oleh kebijakan.”

Note

Anda harus menentukan pengaturan privasi yang sama untuk kontak administratif, pendaftar, teknis, dan penagihan.

Jika Anda memilih Jangan sembunyikan informasi kontak, Anda akan mendapatkan lebih banyak spam email di alamat email yang telah ditentukan.

Siapa pun dapat mengirim kueri WHOIS untuk domain dan mendapatkan kembali semua informasi kontak untuk domain tersebut. Perintah WHOIS tersedia di banyak sistem operasi, dan juga tersedia sebagai aplikasi web di banyak situs web.

Important

Meskipun ada pengguna yang sah untuk informasi kontak yang terkait dengan domain Anda, pengguna yang paling umum adalah spammer, yang menargetkan kontak domain dengan email yang tidak diinginkan dan penawaran palsu. Secara umum, kami menyarankan Anda untuk memilih Hide contact information (Sembunyikan informasi kontak) untuk Perlindungan Privasi.

Untuk mengaktifkan atau menonaktifkan perlindungan privasi untuk beberapa domain, Anda harus membuka kasus dukungan dan meminta perlindungan privasi.

Untuk informasi selengkapnya tentang perlindungan privasi, lihat topik berikut:

- [Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain](#)
- [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Perpanjangan Otomatis (Hanya tersedia saat mengedit pengaturan domain)

Apakah Anda ingin Route 53 memperbarui domain secara otomatis sebelum kedaluwarsa. Biaya pendaftaran dibebankan ke AWS akun Anda. Di konsol lama pengaturan ini hanya tersedia saat

mengedit pengaturan domain. Untuk informasi selengkapnya, lihat [Memperbarui pendaftaran untuk domain](#).

 Important

Jika Anda menonaktifkan perpanjangan otomatis, pendaftaran domain tidak akan diperpanjang saat tanggal kedaluwarsa berlalu, dan Anda mungkin kehilangan kendali atas nama domain.

Periode di mana Anda dapat memperbarui nama domain bervariasi menurut domain tingkat atas (TLD). Untuk ikhtisar tentang memperbarui domain, lihat [Memperbarui pendaftaran untuk domain](#). Untuk informasi tentang memperpanjang pendaftaran domain untuk beberapa tahun tertentu, lihat [Memperpanjang masa pendaftaran untuk domain](#).

Nilai yang dikembalikan Amazon Route 53 saat Anda mendaftarkan domain

Saat Anda mendaftarkan domain Anda dengan Amazon Route 53, Route 53 mengembalikan nilai berikut selain nilai yang Anda tentukan.

Terdaftar di

Tanggal dimana domain awalnya terdaftar dengan Route 53.

Kedaluwarsa pada

Tanggal dan waktu berakhirnya periode pendaftaran saat ini, dalam Greenwich Mean Time (GMT).

Periode pendaftaran biasanya satu tahun, meskipun pendaftar untuk beberapa domain tingkat atas (TLDs) memiliki periode pendaftaran yang lebih lama. Untuk masa pendaftaran dan perpanjangan TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Untuk sebagian besar TLDs, Anda dapat memperpanjang periode pendaftaran hingga sepuluh tahun. Untuk informasi selengkapnya, lihat [Memperpanjang masa pendaftaran untuk domain](#).

Kode status nama domain

Status domain saat ini.

ICANN, organisasi yang mengelola basis data pusat nama domain, telah mengembangkan satu set kode status nama domain (juga dikenal sebagai kode status EPP) yang memberi tahu Anda

status berbagai operasi pada nama domain. Misalnya, mendaftarkan nama domain, mentransfer nama domain ke registrar lain, memperbarui pendaftaran untuk nama domain, dan sebagainya. Semua pendaftar menggunakan set kode status yang sama ini.

Untuk daftar kode status nama domain saat ini dan penjelasan tentang arti setiap kode, kunjungi [situs web ICANN](#) dan cari kode status epp. (Penelusuran di situs web ICANN; penelusuran web terkadang mengembalikan versi dokumen yang lama.)

Kunci transfer

Apakah domain dikunci untuk mengurangi kemungkinan seseorang mentransfer domain Anda ke registrar lain tanpa izin Anda. Jika domain terkunci, nilai Transfer Lock On. Jika domain tidak terkunci, nilainya Mati.

Perpanjangan otomatis

Apakah Route 53 akan secara otomatis memperbarui pendaftaran untuk domain ini sesaat sebelum tanggal kedaluwarsa.

Kode otorisasi

Kode yang diperlukan jika Anda ingin mentransfer pendaftaran domain ini ke registrar lain. Kode otorisasi hanya dibuat jika Anda memintanya. Untuk informasi tentang mentransfer domain ke registrar lain, lihat [Mentransfer domain dari Amazon Route 53 ke registrar lain](#).

Server nama

Server Route 53 yang merespons permintaan DNS untuk domain ini. Sebaiknya Anda tidak menghapus server nama Route 53.

Untuk informasi tentang menambahkan, mengubah, atau menghapus server nama, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

Melihat status pendaftaran domain

ICANN, organisasi yang memelihara basis data pusat nama domain, telah mengembangkan satu set kode status nama domain (juga dikenal sebagai kode status EPP) yang memberi tahu Anda status berbagai operasi, misalnya, mendaftarkan nama domain, mentransfer nama domain ke registrar lain, memperbarui pendaftaran nama domain, dan seterusnya. Semua pendaftar menggunakan set kode status yang sama ini.

Untuk melihat kode status domain Anda, lakukan prosedur berikut ini.

Untuk melihat kode status ICANN domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, perluas Domain dan pilih Domain Terdaftar.
3. Pilih nama domain yang ditautkan.
4. Jika Anda perlu mengambil tindakan, seperti mengirim ulang email verifikasi ke kontak pendaftar, spanduk di atas halaman akan menunjukkan tindakan yang perlu Anda ambil.
5. Untuk status domain Anda saat ini, lihat nilai bidang kode status Domain.

Untuk daftar kode status nama domain saat ini dan penjelasan tentang arti setiap kode, kunjungi [situs web ICANN](#) dan cari kode status epp. (Penelusuran di situs web ICANN; penelusuran web terkadang mengembalikan versi dokumen yang lama.)

Anda juga dapat melihat status pendaftaran di halaman Permintaan.

Untuk melihat status pendaftaran

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, perluas Domain dan pilih Permintaan.
3. Pada halaman Permintaan, Anda dapat melihat status pendaftaran, dan juga status tindakan lain, seperti menghapus domain,, mengunci transfer domain, menambah atau menghapus kunci DNSSEC, yang telah Anda ambil pada domain,

Tindakan apa pun yang mungkin harus Anda ambil untuk menyelesaikan proses, seperti memverifikasi email Anda, juga tercantum.

- Untuk menanggapi permintaan tindakan, pilih tombol radio di sebelah nama domain dan kemudian pilih tindakan dari drop-down Tindakan.

Memperbarui pengaturan domain

Bagian ini memberikan informasi tentang topik-topik berikut yang terkait dengan pengelolaan pengaturan domain di Route 53:

1. [Memperbarui informasi kontak dan kepemilikan domain:](#)

- Pelajari cara memperbarui informasi kontak untuk domain, termasuk kontak administratif, teknis, pendaftar, dan penagihan.
 - Memahami proses untuk mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain.
2. [Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain:](#)
 - Temukan cara mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak, yang menyembunyikan atau mengungkapkan detail pribadi Anda dari pertanyaan WHOIS.
 3. [Mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain:](#)
 - Cari tahu cara mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain, yang menentukan apakah Route 53 secara otomatis memperbarui pendaftaran sebelum kedaluwarsa.
 4. [Mengunci domain untuk mencegah transfer tidak sah ke registrar lain:](#)
 - Pelajari cara mengunci domain untuk mencegah transfer tidak sah ke registrar lain, dan cara menonaktifkan kunci saat diperlukan.
 5. [Memperpanjang masa pendaftaran untuk domain:](#)
 - Memahami proses untuk memperpanjang periode pendaftaran untuk domain, biasanya hingga sepuluh tahun dalam peningkatan satu tahun.
 6. [Memperbarui server nama untuk menggunakan registrar lain](#) dan [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain:](#)
 - Temukan cara memperbarui server nama untuk menggunakan layanan DNS lain atau mengonfigurasi server nama label putih (vanity).
 - Pelajari tentang pertimbangan dan praktik terbaik saat mengganti server nama dan catatan lem.

Memperbarui informasi kontak dan kepemilikan domain

Untuk kontak administratif dan teknis untuk domain, Anda dapat mengubah semua informasi kontak tanpa harus mengotorisasi perubahan. Untuk informasi selengkapnya, lihat [Memperbarui informasi kontak untuk domain](#).

Untuk kontak pendaftar, Anda dapat mengubah sebagian besar nilai tanpa harus mengotorisasi perubahan. Namun, bagi sebagian orang TLDs, mengubah pemilik domain memerlukan otorisasi. Untuk informasi selengkapnya, lihat topik yang berlaku.

Topik

- [Apa yang memicu perubahan kepemilikan domain?](#)

- [TLDs yang membutuhkan pemrosesan khusus untuk mengubah pemilik](#)
- [Memperbarui informasi kontak untuk domain](#)
- [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#)

Apa yang memicu perubahan kepemilikan domain?

Important

Kontak yang Anda cantumkan sebagai pendaftar akan memiliki hak tertentu sebagai Pemegang Nama Terdaftar untuk nama domain, berdasarkan [Kebijakan Transfer ICANN](#). Sebagian besar domain akan dihapus setelah penutupan Anda Akun AWS (untuk informasi lebih lanjut, lihat [AWS Akun saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53](#)), namun jika domain tetap berada di akun tertutup, kontak yang Anda daftarkan sebagai pendaftar mungkin memiliki kemampuan untuk meminta transfer nama domain ke pencatat eksternal. Oleh karena itu, kontak pendaftar yang Anda cantumkan sebaiknya adalah diri Anda sendiri atau orang lain yang Anda percayai untuk bertindak secara bertanggung jawab.

Perubahan berikut pada informasi kontak pendaftar memicu proses perubahan kepemilikan domain:

Untuk tipe kontak Orang

Mengubah bidang Nama Depan atau Nama Belakang memicu perubahan kepemilikan.

Untuk tipe kontak non-orang (Perusahaan, Asosiasi, Badan Publik)

Mengubah bidang Organisasi memicu perubahan kepemilikan.

Pemicu tambahan (semua jenis kontak)

Bergantung pada persyaratan TLD domain Anda, perubahan bidang kontak lainnya juga dapat memicu proses perubahan kepemilikan, termasuk:

- Perubahan pada alamat email pendaftar
- Perubahan pada bidang informasi pengenalan lainnya

Bidang spesifik yang memicu perubahan kepemilikan bervariasi menurut TLD dan ditentukan oleh kebijakan registri domain.

 Warning

Risiko gangguan layanan: Ketika perubahan kepemilikan dipicu, Anda akan menerima email otorisasi. Jika Anda tidak menanggapi email ini dalam waktu 3-15 hari (tergantung pada TLD Anda), pendaftaran domain Anda akan dibatalkan seperti yang dipersyaratkan oleh ICANN, yang akan mengganggu situs web dan layanan email Anda.

Selalu pastikan Anda dapat mengakses alamat email kontak pendaftar sebelum melakukan perubahan kontak.

Perhatikan hal berikut tentang mengubah pemilik domain:

- Bagi sebagian orang TLDs, ada biaya untuk mengubah pemilik domain. Untuk menentukan apakah ada biaya TLD untuk domain Anda, lihat kolom "Ubah Harga Kepemilikan" di [Harga Amazon Route 53 untuk Pendaftaran Domain](#).

 Note

Anda tidak dapat menggunakan AWS kredit untuk membayar biaya, jika ada, untuk mengubah pemilik domain.

- Bagi sebagian orang TLDs, ketika Anda mengubah pemilik domain, kami mengirimkan email otorisasi ke alamat email untuk kontak pendaftar. Kontak pendaftar harus mengikuti petunjuk dalam email untuk mengotorisasi perubahan tersebut.
- Untuk beberapa orang TLDs, Anda perlu mengisi Formulir Perubahan Kepemilikan Domain dan memberikan bukti identitas sehingga insinyur dukungan Amazon Route 53 dapat memperbarui nilai untuk Anda. Jika TLD untuk domain Anda memerlukan formulir Perubahan Kepemilikan Domain, konsol akan menampilkan pesan yang menautkan ke formulir untuk membuka kasus dukungan. Untuk informasi selengkapnya, lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

TLDs yang membutuhkan pemrosesan khusus untuk mengubah pemilik

Ketika Anda mengubah pemilik domain, pendaftar untuk beberapa TLDs memerlukan pemrosesan khusus. Jika Anda mengubah pemilik untuk salah satu domain berikut, lakukan prosedur yang berlaku. Jika Anda mengubah pemilik untuk domain lain, Anda dapat mengubah pemiliknya sendiri,

baik secara terprogram atau menggunakan konsol Route 53. Lihat [Memperbarui informasi kontak untuk domain](#).

Berikut ini TLDs memerlukan pemrosesan khusus untuk mengubah pemilik domain:

[.be](#), [.cl](#), [.com.br](#), [.es](#), [.fi](#), [.ru](#), [.se](#), [.sh](#)

[.be](#)

Anda harus mendapatkan kode transfer dari registri untuk domain.be, dan kemudian membuka case dengan Support AWS .

- Untuk mendapatkan kode transfer, lihat <https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer>, dan ikuti petunjuknya.
- Untuk membuka kasus, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

[.cl](#)

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

[.com.ar](#)

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

[.com.br](#)

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

[.es](#)

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

[.fi](#)

Memulai perubahan pemilik pada konsol Route 53. Setelah Anda memulai perubahan, Anda akan menerima kunci transfer Holder dari alamat email `fi-domain-tech@traficom.fi`. Setelah Anda menerima kunci, buka kasus AWS dukungan dengan Support, dan bagikan kode kunci dengan kami. Lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

.qa

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

.ru

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

.se

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

.sh

Anda harus mengisi dan mengirimkan formulir ke AWS Support. Lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#).

Memperbarui informasi kontak untuk domain

Untuk memperbarui informasi kontak untuk domain, lakukan prosedur berikut.

Warning

Risiko gangguan layanan: Jika perubahan kontak Anda memicu proses perubahan pemilik, Anda akan menerima email otorisasi. Jika Anda tidak menanggapi email ini dalam waktu 3-15 hari (tergantung pada TLD Anda), pendaftaran domain Anda akan dibatalkan seperti yang dipersyaratkan oleh ICANN, yang akan mengganggu situs web dan layanan email Anda. Pastikan Anda dapat mengakses alamat email kontak pendaftar sebelum melakukan perubahan kontak.

Sebelum memperbarui kontak domain

Sebelum membuat perubahan apa pun pada informasi kontak pendaftar domain Anda, lengkapi daftar periksa ini:

1. ☐ Verifikasi akses email - Konfirmasikan bahwa Anda dapat menerima email di alamat email pendaftar saat ini

2. ☐ Memahami pemicu perubahan pemilik - Tinjau [the section called “Apa yang memicu perubahan kepemilikan domain?”](#) untuk memahami perubahan apa yang dapat memicu proses perubahan pemilik
3. ☐ Rencanakan potensi downtime - Jika perubahan pemilik dipicu, Anda memiliki waktu 3-15 hari untuk menanggapi email otorisasi atau domain Anda akan dibatalkan

Untuk memperbarui informasi kontak untuk domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pilih nama domain yang informasi kontaknya ingin Anda perbarui.
4. Di tab Informasi kontak, pilih Edit.
5. Jika Anda tidak memiliki akses ke alamat email untuk kontak pendaftar, lakukan langkah-langkah berikut. Jika Anda memiliki akses ke alamat email untuk kontak pendaftar, lewati ke langkah 6.
 - a. Ubah hanya alamat email untuk kontak pendaftar. Jangan ubah nilai lain untuk kontak mana pun untuk domain. Jika Anda juga ingin mengubah nilai lain, Anda mengubahnya nanti dalam proses.

Pilih Simpan perubahan.

Untuk memverifikasi alamat email baru, kami mengirim email verifikasi ke alamat baru (jika diperlukan untuk TLD). Anda harus memilih tautan di email untuk memverifikasi bahwa alamat email baru itu valid. Jika verifikasi diperlukan, dan Anda tidak memverifikasi alamat email baru, Route 53 menangguhkan domain seperti yang dipersyaratkan oleh ICANN.

Jika Anda perlu mengirim ulang email verifikasi, navigasikan ke halaman Domain terdaftar, pilih tombol radio di sebelah nama domain yang Anda perbarui, dan pilih nama domain yang Anda perbarui. Pada Verifikasi email Anda untuk menghindari peringatan penangguhan domain, pilih Kirim email lagi.

- b. Jika Anda ingin mengubah nilai lain untuk pendaftar, admin, teknologi, atau kontak penagihan untuk domain, kembali ke langkah 1 dan ulangi prosedur.
6. Perbarui nilai yang berlaku. Anda juga dapat memilih Salin kontak pendaftar untuk secara otomatis mengisi informasi yang sama yang Anda masukkan untuk kontak pendaftar. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat mendaftar atau mentransfer domain](#).

Bergantung pada TLD untuk domain Anda dan nilai yang Anda ubah, konsol mungkin menampilkan pesan berikut:

"Untuk mengubah nama atau organisasi pendaftar, buka kasus."

Jika Anda melihat pesan tersebut, lewati sisa prosedur ini dan lihat [Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain](#) untuk informasi lebih lanjut.

7. Pilih Simpan.
8. Jika Anda mengubah pemilik domain, seperti yang dijelaskan di [Apa yang memicu perubahan kepemilikan domain?](#), kami mengirim email ke kontak pendaftar untuk domain tersebut. Email meminta otorisasi untuk perubahan pemilik.

Jika kami tidak menerima otorisasi untuk perubahan dalam waktu 3 hingga 15 hari, bergantung pada domain level teratas, kami harus membatalkan permintaan seperti yang diwajibkan oleh ICANN.

Email berasal dari salah satu alamat email berikut.

TLDs	Alamat email asal email otorisasi
.fr	nic@nic.fr
.com.id .net.au	noreply@emailverification.info
Semua yang lain	Salah satu alamat email berikut: - noreply@registrar.amazon - noreply@domainnameverification.net - noreply@emailverification.info

9. Jika Anda mengalami masalah saat memperbarui informasi kontak, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Untuk informasi tentang API yang dapat Anda gunakan untuk memperbarui informasi kontak, lihat [UpdateDomainContact](#).

Mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain

Jika registri untuk domain Anda mengharuskan Anda untuk melengkapi Perubahan Kepemilikan Domain dan mengirimkan formulir ke AWS Support, lakukan prosedur berikut. Untuk menentukan apakah Anda perlu melakukan prosedur ini, lihat topik berikut:

- Untuk menentukan apakah nilai yang Anda ubah dianggap sebagai perubahan pemilik, lihat [Apa yang memicu perubahan kepemilikan domain?](#).
- Untuk menentukan apakah formulir Perubahan Kepemilikan Domain diperlukan untuk domain Anda, lihat [TLDs yang membutuhkan pemrosesan khusus untuk mengubah pemilik](#).

Untuk mengubah pemilik domain ketika registri memerlukan formulir Perubahan Kepemilikan Domain

1. Lihat pengantar topik ini untuk menentukan apakah registri untuk domain Anda memerlukan pemrosesan khusus untuk mengubah pemilik domain. Jika demikian, dan jika formulir Perubahan Kepemilikan Domain diperlukan, lanjutkan dengan prosedur ini.

Jika formulir Perubahan Kepemilikan Domain tidak diperlukan, lakukan prosedur di topik yang berlaku.

2. Unduh [Perubahan Formulir Kepemilikan Domain](#). File dikompresi menjadi file .zip.
3. Isi formulirnya.
4. Untuk kontak pendaftar untuk mantan pemilik domain dan untuk pemilik baru, dapatkan salinan bukti identitas yang ditandatangani (kartu identitas, SIM, paspor, atau bukti identitas resmi lainnya).

Selain itu, jika badan hukum terdaftar sebagai organisasi pendaftar, kumpulkan informasi berikut untuk pemilik domain sebelumnya dan pemilik baru:

- Bukti bahwa organisasi tempat domain terdaftar ada.

- Bukti bahwa perwakilan pemilik lama dan pemilik baru berwenang untuk bertindak atas nama organisasi. Dokumen ini harus merupakan dokumen legal bersertifikat yang berisi nama organisasi dan nama perwakilan sebagai pejabat penandatanganan (misalnya, CEO, Presiden, atau Direktur Eksekutif).
5. Pindai formulir Perubahan Kepemilikan Domain dan bukti yang diperlukan. Simpan dokumen yang dipindai dalam format umum, seperti file .pdf atau file .png.
 6. Dengan menggunakan AWS akun tempat domain saat ini terdaftar, masuk ke [AWS Support Center](#).

 Important

Anda harus masuk baik dengan menggunakan akun root atau dengan menggunakan pengguna yang telah diberikan izin IAM dalam satu atau beberapa cara berikut:

- Pengguna diberi kebijakan AdministratorAccess terkelola.
- Pengguna diberi AmazonRoute53 kebijakan DomainsFullAccess terkelola.
- Pengguna diberi AmazonRoute53 kebijakan FullAccess terkelola.

Jika Anda tidak masuk dengan menggunakan akun root atau dengan menggunakan pengguna yang memiliki izin yang diperlukan, kami tidak dapat memperbarui pemilik domain. Persyaratan ini mencegah pengguna yang tidak sah mengubah pemilik domain.

7. Tentukan nilai-nilai berikut ini:

Mengenai

Terima nilai default Akun dan penagihan.

Layanan

Terima nilai default Domain.

Kategori

Terima nilai default Perubahan Kepemilikan.

Kepelikan

Terima nilai default pertanyaan Umum.

Pilih Langkah selanjutnya: Informasi tambahan

Subjek

Tentukan Ubah pemilik domain.

Deskripsi

Berikan informasi berikut ini:

- Domain yang ingin Anda ubah pemiliknya
- [12 digit ID akun](#) dari AWS akun tempat domain terdaftar

Tambahkan lampiran

Unggah dokumen yang Anda pindai di langkah 5.

Metode kontak

Tentukan metode kontak dan masukkan nilai yang berlaku.

8. Pilih Kirim.

Insinyur AWS Support meninjau informasi yang Anda berikan dan memperbarui pengaturan. Teknisi akan menghubungi Anda saat pembaruan selesai atau menghubungi Anda untuk informasi lebih lanjut.

Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain

Saat Anda mendaftarkan domain dengan Amazon Route 53 atau mentransfer domain ke Route 53, kami mengaktifkan perlindungan privasi secara default untuk semua kontak untuk domain tersebut. Ini biasanya menyembunyikan sebagian besar informasi kontak Anda dari kueri WHOIS ("Siapa") dan mengurangi jumlah spam yang Anda terima. Ketika Anda mengaktifkan perlindungan privasi, informasi kontak Anda diganti dengan informasi kontak untuk registrar atau dengan frasa "REDACTED FOR PRIVACY", atau "Atas nama <domain name>pemilik."

Jika Anda memilih untuk menonaktifkan perlindungan privasi, Anda harus menonaktifkannya untuk semua kontak untuk domain. Jika Anda menonaktifkan perlindungan privasi, siapa pun dapat mengirim kueri WHOIS untuk domain tersebut dan, untuk sebagian besar domain tingkat atas (TLDs), mungkin bisa mendapatkan semua informasi kontak yang Anda berikan saat Anda mendaftarkan atau mentransfer domain, termasuk nama, alamat, nomor telepon, dan alamat email. Perintah

WHOIS tersedia secara luas; ini termasuk dalam banyak sistem operasi, dan juga tersedia sebagai aplikasi web di banyak situs web.

Jika Anda mentransfer domain ke pencatat lain, dan perlindungan privasi diaktifkan untuk kontak domain, email untuk memverifikasi transfer akan dikirimkan dari alamat identity-protect.org untuk terdaftar di Amazon Registrar. TLDs Untuk menentukan registrar TLD Anda, lihat [Menemukan registrar Anda](#).

Informasi yang dapat Anda sembunyikan dari permintaan WHOIS tergantung pada dua faktor utama:

Registri untuk domain tingkat atas

Sebagian besar pendaftar TLD menyembunyikan semua informasi kontak secara otomatis, beberapa memungkinkan Anda memilih untuk menyembunyikan semua informasi kontak, beberapa mengizinkan Anda menyembunyikan hanya beberapa informasi, dan beberapa tidak mengizinkan Anda menyembunyikan informasi apa pun. Beberapa pendaftar TLD sengaja menekan perlindungan privasi untuk mematuhi peraturan setempat atau kebijakan registri.

Ketika perlindungan privasi pada domain diaktifkan, informasi kontak Anda diganti dengan informasi kontak untuk layanan perlindungan privasi, atau dengan frasa "REDACTED FOR PRIVACY." Layanan perlindungan privasi menerapkan fitur pencegahan spam (rotasi dan SPF/DKIM/spam analisis alamat) dan akan, dalam banyak kasus, secara otomatis meneruskan email yang melewati filter ini. Namun, tidak disarankan untuk mengirim email penting ke alamat email yang dilindungi privasi karena mekanisme spam dapat mencegahnya diteruskan.

Selain itu, pilihan mekanisme perlindungan privasi yang digunakan untuk domain tidak dapat dikonfigurasi dan dipilih secara otomatis oleh sistem. Detail kontak untuk layanan perlindungan privasi kami tidak dapat diperbarui secara manual.

Note

Untuk mengaktifkan atau menonaktifkan perlindungan privasi untuk beberapa domain, Anda harus membuka kasus dukungan dan meminta perlindungan privasi. Untuk informasi lebih lanjut, lihat bagian yang berlaku di [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#):

- [.co.uk \(Britania Raya\)](#)
- [.me.uk \(Britania Raya\)](#)
- [.org.uk \(Britania Raya\)](#)

- [.tautan](#)

Registrar

Saat Anda mendaftarkan domain dengan Route 53 atau mentransfer domain ke Route 53, registrar untuk domain tersebut adalah Amazon Registrar atau rekan registrar kami, Gandi. Amazon Registrar dan Gandi menyembunyikan informasi yang berbeda secara default:

- Registrar Amazon— Secara default, semua informasi kontak Anda disembunyikan. Namun, peraturan untuk registri TLD diutamakan.
- Gandi— Secara default, semua informasi kontak Anda disembunyikan kecuali nama organisasi, jika ada. Namun, peraturan untuk registri TLD diutamakan.

Untuk [geografis TLDs](#) yang tidak memungkinkan perlindungan privasi, informasi pribadi Anda akan ditandai sebagai “disunting” pada halaman [Pencarian Direktori Whois](#) di situs web Gandi. Namun, informasi pribadi Anda mungkin tersedia di registri domain atau di situs web WHOIS pihak ketiga.

Untuk mengetahui informasi apa yang tersembunyi untuk TLD untuk domain Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Saat Anda ingin mengaktifkan atau menonaktifkan perlindungan privasi untuk domain yang Anda daftarkan menggunakan Route 53, lakukan prosedur berikut.

Important

Ketersediaan perlindungan privasi: Perlindungan privasi tidak tersedia untuk semua TLDs. Umum TLDs yang tidak mendukung perlindungan privasi termasuk .de, .us, .com.au, .es, dan beberapa lainnya.

Jika Anda tidak melihat bagian “Perlindungan privasi” saat mengedit informasi kontak domain Anda, perlindungan privasi tidak didukung untuk TLD domain Anda.

Untuk daftar lengkap TLDs yang tidak mendukung perlindungan privasi, lihat [TLDs yang tidak mendukung perlindungan privasi](#). Untuk informasi terperinci tentang dukungan perlindungan privasi untuk TLD apa pun, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Untuk mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pilih nama domain yang ingin Anda aktifkan atau nonaktifkan perlindungan privasinya.
4. Di bagian Informasi kontak, pilih Edit.
5. Di bagian Perlindungan privasi, pilih apakah akan menyembunyikan informasi kontak. Anda harus menentukan pengaturan privasi yang sama untuk keempat kontak: admin, pendaftar, teknis, dan penagihan.

 Note

Jika bagian Perlindungan privasi tidak ditampilkan, perlindungan privasi tidak didukung untuk TLD domain Anda. Informasi kontak Anda akan terlihat publik di kueri WHOIS untuk domain yang tidak mendukung perlindungan privasi.

6. Pilih Simpan perubahan.
7. Jika Anda mengalami masalah saat mengaktifkan atau menonaktifkan perlindungan privasi, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

TLDs yang tidak mendukung perlindungan privasi

Berikut ini TLDs tidak mendukung perlindungan privasi. Jika domain Anda menggunakan salah satu dari ini TLDs, informasi kontak Anda akan terlihat publik di kueri WHOIS:

Generik TLDs

.audio, .ceo, .diet, .flowers, .guitars, .hosting, .juegos, .property, .sexy

Geografis TLDs

.cl (Chili), .com.ar (Argentina), .com.au (Australia), .com.br (Brasil), .com.sg (Singapura), .de (Jerman), .es (Spanyol), .in (India), .net.au (Australia), .qa (Qatar), .ru (Rusia), .sg (Singapura), .us (Amerika Serikat), .vg (Kepulauan Virgin Britania Raya)

 Note

Daftar ini mencakup yang paling umum TLDs yang tidak mendukung perlindungan privasi. Untuk informasi lengkap dan up-to-date informasi tentang dukungan perlindungan privasi untuk TLD tertentu, lihat halaman TLD individual di [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Memecahkan masalah perlindungan privasi

Opsi perlindungan privasi tidak tersedia di konsol

Ini menunjukkan bahwa TLD domain Anda tidak mendukung perlindungan privasi. Informasi kontak Anda akan terlihat publik di kueri WHOIS. Ini adalah perilaku normal tertentu TLDs karena kebijakan registri atau peraturan setempat.

Untuk memverifikasi apakah TLD Anda mendukung perlindungan privasi, periksa halaman TLD individual di [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#) atau lihat [TLDs yang tidak mendukung perlindungan privasi](#)

Informasi kontak masih terlihat setelah mengaktifkan perlindungan privasi

Beberapa pendaftar mempertahankan basis data WHOIS mereka sendiri dan dapat terus menampilkan informasi kontak bahkan ketika perlindungan privasi diaktifkan dengan Route 53. Ini dikendalikan oleh registri TLD, bukan oleh Route 53.

Selain itu, beberapa pendaftar TLD sengaja mempertahankan perlindungan privasi terbatas atau layanan redaksi untuk domain mereka.

Mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain

Saat Anda ingin mengubah apakah Amazon Route 53 secara otomatis memperbarui pendaftaran untuk domain sesaat sebelum tanggal kedaluwarsa, atau Anda ingin melihat pengaturan saat ini untuk pembaruan otomatis, lakukan prosedur berikut.

Perhatikan bahwa Anda tidak dapat menggunakan AWS kredit untuk membayar biaya perpanjangan pendaftaran domain.

 Note

Pastikan Anda mematikan perpanjangan otomatis jika Anda berniat untuk membatalkan AWS akun Anda. Jika tidak, Anda akan terus menerima pemberitahuan pembaruan dari AWS. Namun, domain Anda tidak akan diperpanjang, kecuali Anda mengaktifkan kembali akun Anda.

Untuk mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pilih nama domain yang ingin Anda perbarui.
4. Pada bagian Detail, di dropdown Tindakan, pilih Aktifkan perpanjangan otomatis

<domain name>Di Aktifkan perpanjangan otomatis untuk? setuju untuk membayar tarif tahunan, dan pilih Aktifkan.

 Note

Harga yang tercantum adalah untuk periode pendaftaran saat ini, dan dapat berubah. Untuk informasi selengkapnya, lihat [Harga Amazon Route 53 untuk Pendaftaran Domain](#).

5. Untuk menonaktifkan perpanjangan otomatis, pilih Matikan perpanjangan otomatis di menu tarik-turun Tindakan.
6. Jika Anda mengalami masalah saat mengaktifkan atau menonaktifkan perpanjangan otomatis, Anda dapat menghubungi Support AWS secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Mengunci domain untuk mencegah transfer tidak sah ke registrar lain

Registries domain untuk semua generik TLDs dan banyak geografis TLDs memungkinkan Anda mengunci domain untuk mencegah seseorang mentransfer domain ke registrar lain tanpa izin Anda. Untuk menentukan apakah registri untuk domain memungkinkan Anda mengunci domain, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#). Jika penguncian didukung dan Anda

ingin mengunci domain Anda, lakukan prosedur berikut. Anda juga dapat menggunakan prosedur untuk menonaktifkan kunci jika Anda ingin mentransfer domain ke registrar lain.

Untuk mengunci domain untuk mencegah transfer tidak sah ke registrar lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Registered Domains (Domain terdaftar).
3. Pilih nama domain yang ingin Anda perbarui.
4. Pada bagian Detail, di dropdown Tindakan, pilih Aktifkan kunci transfer atau Matikan kunci transfer, tergantung pada apakah Anda ingin mengaktifkan atau menonaktifkan kunci transfer.

Anda dapat menavigasi ke halaman Permintaan untuk melihat kemajuan permintaan Anda.

5. Jika Anda mengalami masalah saat mengunci domain, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Dalam pencarian WHOIS, status ini muncul sebagai:clientTransferProhibited. Beberapa TLDs mungkin memiliki status ini sebagai tambahan:

- clientUpdateProhibited
- clientDeleteProhibited

Memperpanjang masa pendaftaran untuk domain

Saat Anda mendaftarkan domain dengan Amazon Route 53 atau Anda mentransfer pendaftaran domain ke Route 53, kami mengonfigurasi domain untuk diperpanjang secara otomatis. Periode perpanjangan otomatis biasanya satu tahun, meskipun pendaftar untuk beberapa domain tingkat atas (TLDs) memiliki periode perpanjangan yang lebih lama.

Perhatikan hal-hal berikut:

Periode perpanjangan maksimal

Semua kode negara umum TLDs dan banyak TLDs memungkinkan Anda memperpanjang pendaftaran domain untuk periode yang lebih lama, biasanya hingga sepuluh tahun dalam peningkatan satu tahun. Untuk menentukan apakah Anda dapat memperpanjang masa

pendaftaran domain, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#). Jika periode pendaftaran yang lebih lama diizinkan, lakukan prosedur berikut.

Batasan kapan Anda dapat memperbarui atau memperpanjang pendaftaran domain

Beberapa pendaftar TLD memiliki batasan kapan Anda dapat memperbarui atau memperpanjang pendaftaran domain, misalnya, dua bulan terakhir sebelum domain kedaluwarsa. Bahkan jika registri mengizinkan perpanjangan periode pendaftaran untuk domain, mereka mungkin tidak mengizinkannya pada jumlah hari saat ini sebelum domain kedaluwarsa.

 Note

Misalnya, jika periode perpanjangan maksimum TLDs yang diizinkan adalah 5 tahun untuk domain Anda, Anda dapat menambahkan perpanjangan tahunan kapan saja hingga Anda mencapai batas 5 tahun. Lebih khusus lagi, jika Anda memiliki domain yang saat ini memiliki validitas 2,5 tahun, Anda hanya dapat memperbaruinya hingga 2 tahun lagi.

AWS kredit

Anda tidak dapat menggunakan AWS kredit untuk membayar biaya untuk memperpanjang periode pendaftaran domain.

Untuk memperpanjang periode pendaftaran domain Anda

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Registered Domains (Domain terdaftar).
3. Pilih nama domain yang ingin Anda perpanjang masa pendaftarannya.
4. Di bagian Detail, di dropdown Tindakan pilih Perbarui pendaftaran domain.
5. Dalam kotak dialog Perbarui pendaftaran domain, di dropdown Periode perpanjangan, pilih jumlah tahun yang ingin Anda perpanjang pendaftarannya.

Daftar tersebut menunjukkan semua opsi saat ini berdasarkan tanggal kedaluwarsa saat ini dan periode pendaftaran maksimum yang diizinkan oleh registri untuk domain ini. Tanggal kedaluwarsa dengan jumlah tahun yang diterapkan tercantum di bawah durasi.

6. Pilih Perbarui pendaftaran domain.

Saat kami menerima konfirmasi dari registri bahwa mereka telah memperbarui tanggal kedaluwarsa Anda, kami mengirim Anda email untuk mengonfirmasi bahwa kami telah mengubah tanggal kedaluwarsa.

7. Jika Anda mengalami masalah saat memperpanjang periode pendaftaran untuk domain, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Memperbarui server nama untuk menggunakan registrar lain

Jika Anda ingin memindahkan manajemen DNS ke registrar lain, Anda perlu memperbarui server nama untuk menunjuk

Untuk memperbarui server nama untuk domain Anda saat Anda ingin menggunakan layanan DNS lain

1. Gunakan proses yang disediakan oleh layanan DNS Anda untuk mendapatkan server nama untuk domain.
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Domain terdaftar.
4. Pilih nama domain yang ingin Anda konfigurasi untuk menggunakan layanan DNS lain.
5. Di bagian Detail, di bawah drop-down Tindakan, pilih Edit server nama.
6. Hapus server nama yang ada, lalu tambahkan nama server nama ke server nama yang Anda dapatkan dari layanan DNS Anda di langkah 1.
7. Pilih Simpan perubahan.
8. (Opsional) Hapus zona yang di-hosting yang dibuat oleh Route 53 secara otomatis saat Anda mendaftarkan domain. Ini mencegah Anda ditagih untuk zona yang di-hosting yang tidak Anda gunakan.
 - a. Pada panel navigasi, pilih Hosted Zones (Zona yang di-hosting).
 - b. Pilih tombol radio untuk zona yang di-hosting yang memiliki nama yang sama dengan domain Anda.
 - c. Pilih Delete Hosted Zone (Hapus Zona yang Di-hosting).

- d. Pilih Confirm (Konfirmasi) untuk mengonfirmasi bahwa Anda ingin menghapus zona yang di-hosting.

Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain

Saat Anda mendaftarkan domain dengan Route 53, kami secara otomatis membuat zona yang di-hosting untuk domain tersebut, menetapkan empat server nama ke zona yang di-hosting, dan kemudian memperbarui pendaftaran domain untuk menggunakan server nama tersebut. Anda biasanya tidak perlu mengubah pengaturan tersebut kecuali jika Anda ingin menggunakan layanan DNS lain atau Anda ingin menggunakan server nama label putih.

Jumlah maksimum server nama per domain di Route 53 adalah 6.

Warning

Jika Anda mengubah server nama ke nilai yang salah, menentukan alamat IP yang salah dalam glue record, atau menghapus satu atau beberapa server nama tanpa menentukan yang baru, situs web atau aplikasi Anda mungkin tidak tersedia di internet hingga dua hari.

Topik

- [Pertimbangan untuk mengubah server nama dan glue record](#)
- [Menambahkan atau mengubah nama server atau glue record](#)

Pertimbangan untuk mengubah server nama dan glue record

Pertimbangkan masalah berikut sebelum Anda mengubah konfigurasi Anda.

Topik

- [You want to make Route 53 the DNS service for your domain](#)
- [You want to use another DNS service](#)
- [You want to use white-label name servers](#)
- [You're changing name servers for a .it domain](#)

Anda ingin menjadikan layanan DNS Route 53 untuk domain Anda

Jika saat ini Anda menggunakan layanan DNS lain dan ingin menjadikan Route 53 sebagai layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#) untuk petunjuk mendetail tentang cara memigrasikan layanan DNS ke Route 53.

Important

Jika Anda tidak mengikuti proses migrasi dengan ketat, domain Anda dapat menjadi tidak tersedia di internet hingga dua hari.

Anda ingin menggunakan layanan DNS lainnya

Jika Anda ingin menggunakan layanan DNS selain Route 53 untuk domain Anda, gunakan prosedur berikut ini untuk mengubah server nama untuk pendaftaran domain ke server nama yang disediakan oleh layanan DNS lainnya.

Note

Jika Anda mengubah server nama dan Route 53 mengembalikan pesan kesalahan berikut, registri untuk TLD tidak mengenali server nama yang Anda tentukan sebagai server nama yang valid:

```
"We're sorry to report that the operation failed after we forwarded your request to our registrar associate. This is because: One or more of the specified name servers are not known to the domain registry."
```

Registri TLD biasanya mendukung server nama yang disediakan oleh layanan DNS publik tetapi tidak mendukung server DNS pribadi, seperti server DNS yang Anda konfigurasi pada EC2 instans Amazon, kecuali registri memiliki alamat IP untuk server nama tersebut. Route 53 tidak mendukung penggunaan server nama yang tidak dikenali oleh registri TLD. Jika Anda mengalami kesalahan ini, Anda harus mengubah ke server nama untuk Route 53 atau layanan DNS publik lainnya.

Anda ingin menggunakan server nama label putih

Jika Anda ingin nama server nama Anda menjadi subdomain dari nama domain Anda, Anda dapat membuat server nama label putih. (Server nama label putih juga dikenal sebagai

server nama vanity atau server nama pribadi.) Misalnya, Anda dapat membuat server nama ns1.example.com melalui ns4.example.com untuk domain example.com. Untuk menggunakan server nama label putih, gunakan prosedur berikut untuk menentukan alamat IP server nama Anda bukan nama. Alamat IP ini dikenal sebagai glue record.

Untuk informasi selengkapnya tentang konfigurasi server nama label putih, lihat [Mengonfigurasi server nama label putih](#).

Anda sedang mengubah server nama untuk domain .it

IName server untuk domain TI Anda harus melewati pemeriksaan DNS. Kami menyarankan agar Anda memeriksa server nama di <https://dns-check.nic.it/> sebelum mengirimkan permintaan perubahan. Registri terus merespons kueri DNS menggunakan server nama sebelum Anda membuat perubahan. Jika server nama sebelumnya tidak lagi tersedia, domain Anda menjadi tidak tersedia di internet.

 Important

Setiap kali Anda mengubah server nama untuk domain, konfirmasi bahwa DNS merespons pertanyaan dengan server nama baru sebelum Anda membatalkan layanan DNS lama atau Anda menghapus zona yang di-hosting Route 53 yang menggunakan server nama lama.

Untuk informasi tentang mendapatkan bantuan AWS untuk memperbaiki nama server nama Anda dengan registri untuk domain.it, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#)

Menambahkan atau mengubah nama server atau glue record

Untuk menambah atau mengubah server nama atau glue record, lakukan prosedur berikut.

 Note

Secara default, DNS resolver biasanya men-cache nama server nama selama dua hari. Akibatnya, perubahan Anda memerlukan waktu dua hari untuk diterapkan. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Untuk menambah atau mengubah server nama atau glue record untuk domain

1. Tinjau [Pertimbangan untuk mengubah server nama dan glue record](#) dan selesaikan masalah yang terjadi, jika ada.
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Domain terdaftar.
4. Pilih nama domain yang ingin Anda edit pengaturannya.
5. Di bagian Detail, di dropdown Tindakan pilih Edit server nama.
6. Dalam kotak dialog Edit server nama, Anda dapat melakukan hal berikut:
 - Ubah layanan DNS untuk domain dengan melakukan salah satu hal berikut:
 - Ganti server nama untuk layanan DNS lain dengan server nama untuk zona yang di-hosting Route 53
 - Ganti server nama untuk zona yang di-hosting Route 53 dengan server nama untuk layanan DNS lain
 - Ganti server nama untuk satu zona yang di-hosting Route 53 dengan server nama untuk zona yang di-hosting Route 53 yang berbeda

Untuk informasi tentang mengubah layanan DNS untuk domain, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#). Untuk informasi tentang mendapatkan server nama untuk zona yang di-hosting Route 53 yang ingin Anda gunakan untuk layanan DNS untuk domain, lihat [Mendapatkan server nama untuk zona yang di-hosting publik](#).

- Tambahkan satu server nama atau lebih.
- Ganti nama server nama yang sudah ada.
- Jika Anda menentukan server nama label putih, tambahkan atau ubah alamat IP dalam glue record. Anda dapat memasukkan alamat dalam IPv4 atau IPv6 format. Jika server nama memiliki beberapa alamat IP, masukkan setiap alamat pada baris terpisah.

Server nama label putih menyertakan nama domain Anda, seperti example.com, dalam nama server nama, seperti ns1.example.com. Saat Anda menentukan server nama label putih, Route 53 meminta Anda untuk menentukan satu atau beberapa alamat IP untuk server nama. Alamat IP dikenal sebagai glue record. Untuk informasi selengkapnya, lihat [Mengonfigurasi server nama label putih](#).

- Menghapus server nama. Pilih ikon x di sisi kanan bidang untuk server nama tersebut.

 Warning

Jika Anda mengubah server nama ke nilai yang salah, menentukan alamat IP yang salah dalam glue record, atau menghapus satu atau beberapa server nama tanpa menentukan yang baru, situs web atau aplikasi Anda mungkin tidak tersedia di internet hingga dua hari.

7. Pilih Perbarui.
8. Jika Anda mengalami masalah saat menambahkan atau mengubah server nama atau catatan lem, Anda dapat menghubungi AWS Support secara gratis. Lihat informasi yang lebih lengkap di [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Memperbarui pendaftaran untuk domain

Saat Anda mendaftarkan domain dengan Amazon Route 53 atau Anda mentransfer pendaftaran domain ke Route 53, kami mengonfigurasi domain untuk diperpanjang secara otomatis. Periode perpanjangan otomatis biasanya satu tahun, meskipun pendaftar untuk beberapa domain tingkat atas (TLDs) memiliki periode perpanjangan yang lebih lama. Untuk masa pendaftaran dan perpanjangan TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

 Note

Anda tidak dapat menggunakan AWS kredit untuk membayar biaya perpanjangan pendaftaran domain.

Untuk sebagian besar domain tingkat atas (TLDs), Anda dapat mengubah tanggal kedaluwarsa domain. Untuk informasi selengkapnya, lihat [Memperpanjang masa pendaftaran untuk domain](#).

 Important

Jika Anda menonaktifkan perpanjangan otomatis, perhatikan efek berikut pada domain Anda:

- Beberapa registri TLD menghapus domain bahkan sebelum tanggal kedaluwarsa jika Anda tidak memperbarui cukup awal. Kami sangat merekomendasikan Anda membiarkan pembaruan otomatis diaktifkan jika Anda ingin mempertahankan nama domain.

- Kami juga sangat merekomendasikan agar Anda tidak berencana untuk mendaftarkan ulang domain setelah masa berlakunya habis. Beberapa registrar mengizinkan orang lain untuk mendaftarkan domain segera setelah domain kedaluwarsa, sehingga Anda mungkin tidak dapat mendaftar ulang sebelum domain diambil oleh orang lain.
- Beberapa registri membebankan biaya premium yang cukup besar untuk memulihkan domain yang kedaluwarsa.
- Pada atau dekat tanggal kedaluwarsa, domain menjadi tidak tersedia di internet.

Untuk menentukan apakah penambahan otomatis diaktifkan untuk domain Anda, lihat [Mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain](#).

Jika perpanjangan otomatis diaktifkan, hal ini akan terjadi:

45 hari sebelum kedaluwarsa

Kami mengirim email ke kontak pendaftar yang memberi tahu Anda bahwa perpanjangan otomatis saat ini diaktifkan dan memberikan petunjuk tentang cara menonaktifkannya. Perbarui alamat email kontak pendaftar Anda agar Anda tidak melewatkan email ini.

35 atau 30 hari sebelum kedaluwarsa

Untuk semua domain kecuali domain.com.ar dan .com.br, kami memperbarui pendaftaran domain 35 hari sebelum tanggal kedaluwarsa sehingga kami memiliki waktu untuk menyelesaikan masalah apa pun dengan perpanjangan Anda sebelum nama domain kedaluwarsa.

Pendaftaran untuk domain.com.ar dan .com.br mengharuskan kami memperbarui domain tidak lebih dari 30 hari sebelum kedaluwarsa. Anda akan mendapatkan email pembaruan dari Gandi, rekan registrar kami, 30 hari sebelum kedaluwarsa, yang merupakan hari yang sama saat kami memperbarui domain Anda jika pembaruan otomatis diaktifkan.

 Note

Saat kami memperbarui domain Anda, kami mengirim Anda email untuk memberi tahu Anda bahwa kami telah memperbaruinya. Jika perpanjangan gagal, kami mengirimkan email kepada Anda untuk menjelaskan alasan kegagalan tersebut.

Jika perpanjangan otomatis dinonaktifkan, inilah yang terjadi saat tanggal kedaluwarsa untuk nama domain semakin dekat:

45 hari sebelum kedaluwarsa

Kami mengirim email ke kontak pendaftar untuk domain yang memberi tahu Anda bahwa perpanjangan otomatis saat ini dinonaktifkan dan memberikan petunjuk tentang cara mengaktifkannya. Perbarui alamat email kontak pendaftar Anda agar Anda tidak melewatkan email ini.

30 hari dan 7 hari sebelum kedaluwarsa

Jika perpanjangan otomatis dinonaktifkan untuk domain, ICANN, badan pengatur untuk pendaftaran domain, mengharuskan registrar untuk mengirimkan email kepada Anda. Email berasal dari salah satu alamat email berikut:

- noreply@registrar.amazon — Untuk domain yang pendaftarnya adalah Amazon Registrar.
- noreply@domainnameverification.net atau noreply@emailverification.info — Untuk domain yang pendaftarnya adalah rekanan registrar kami, Gandi.

Untuk menentukan registrar TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Jika Anda mengaktifkan perpanjangan otomatis kurang dari 30 hari sebelum kedaluwarsa, dan periode perpanjangan belum berlalu, kami memperbarui domain dalam waktu 24 jam.

Important

Beberapa pendaftar TLD memiliki batasan kapan Anda dapat memperbarui domain. Untuk detail khusus untuk domain Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#). Selain itu, pemrosesan perpanjangan bisa memakan waktu hingga satu hari. Jika Anda menunda terlalu lama sebelum mengaktifkan perpanjangan otomatis, domain mungkin kedaluwarsa sebelum perpanjangan dapat diproses, dan Anda mungkin kehilangan domain. Jika tanggal kedaluwarsa semakin dekat, sebaiknya Anda memperpanjang tanggal kedaluwarsa domain secara manual. Untuk informasi selengkapnya, lihat [Memperpanjang masa pendaftaran untuk domain](#).

Untuk informasi selengkapnya tentang periode perpanjangan, lihat bagian [Tenggat waktu untuk memperbarui dan memulihkan domain untuk TLD Anda](#). [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Setelah tanggal kedaluwarsa

Registrar memegang sebagian besar domain untuk waktu yang singkat setelah kedaluwarsa, sehingga Anda mungkin dapat memperbarui domain kedaluwarsa setelah tanggal kedaluwarsa, tetapi jika Anda ingin mempertahankan domain Anda, kami sangat menyarankan agar Anda tetap mengaktifkan pembaruan otomatis. Untuk informasi tentang cara memperbarui domain setelah tanggal kedaluwarsa, lihat [Memulihkan domain yang kedaluwarsa atau dihapus](#).

Jika domain Anda kedaluwarsa tetapi perpanjangan terlambat diizinkan untuk domain, Anda dapat memperbarui domain dengan harga perpanjangan standar. Untuk menentukan apakah domain masih dalam periode perpanjangan akhir, lakukan prosedur di bagian [Memperpanjang masa pendaftaran untuk domain](#). Jika domain masih terdaftar, itu dalam periode perpanjangan akhir.

Untuk informasi selengkapnya tentang periode perpanjangan, lihat bagian [Tenggat waktu untuk memperbarui dan memulihkan domain untuk TLD Anda](#). [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Memulihkan domain yang kedaluwarsa atau dihapus

Jika Anda tidak memperbarui domain sebelum akhir periode perpanjangan akhir atau jika Anda secara tidak sengaja menghapus domain, untuk beberapa pendaftar untuk domain tingkat atas (TLDs), Anda dapat memulihkan domain sebelum tersedia bagi orang lain untuk mendaftar.

Saat domain dihapus atau melewati akhir periode perpanjangan akhir, domain tidak lagi muncul di konsol Amazon Route 53.

Important

Harga untuk memulihkan domain biasanya lebih tinggi dan terkadang jauh lebih tinggi daripada harga untuk mendaftarkan atau memperbarui domain. Untuk harga saat ini untuk memulihkan domain, lihat kolom Harga Pemulihan di [Amazon Route 53 Harga untuk Pendaftaran Domain](#).

Anda tidak dapat menggunakan AWS kredit untuk membayar biaya pemulihan domain yang kedaluwarsa.

Untuk mencoba memulihkan pendaftaran domain ketika domain dihapus atau periode perpanjangan akhir telah kedaluwarsa

1. Tentukan apakah registri TLD untuk domain mendukung pemulihan domain dan, jika demikian, periode selama pemulihan diizinkan.

- a. Kunjungi [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

 Important

Untuk domain TLD generik yang dihapus dalam 5 hari pertama setelah pendaftaran, periode penukaran standar 30 hari (untuk memeriksa jumlah hari penukaran aktual, lihat) tidak berlaku. [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#) Sebaliknya, domain ini segera tersedia untuk pendaftaran baru.

- b. Temukan TLD untuk domain Anda, dan tinjau nilainya di bagian Tenggat waktu untuk memperbarui dan memulihkan domain.

 Important

Kami meneruskan permintaan restorasi ke Gandi, yang memproses permintaan selama jam kerja Senin sampai Jumat. Gandi berbasis di Paris, di mana waktunya UTC/GMT +1 jam. Akibatnya, bergantung pada waktu Anda mengirimkan permintaan, dalam kasus yang jarang terjadi, diperlukan waktu seminggu atau lebih untuk memproses permintaan.

2. Tinjau harga untuk memulihkan domain, yang sering kali lebih tinggi dan terkadang jauh lebih tinggi daripada harga untuk mendaftarkan atau memperbarui domain. Di [Amazon Route 53 Harga untuk Pendaftaran Domain](#), temukan TLD untuk domain Anda (seperti.com) dan periksa harganya di kolom Harga Pemulihan. Jika Anda masih ingin memulihkan domain, perhatikan harganya; Anda akan membutuhkannya di langkah selanjutnya.
3. Dengan menggunakan AWS akun tempat domain terdaftar, masuk ke [AWS Support Center](#).
4. Tentukan nilai-nilai berikut ini:

Mengenai

Terima nilai default Akun dan penagihan.

Layanan

Terima nilai default Domain.

Kategori

Terima nilai default Restorasi.

Kepelikan

Terima nilai default pertanyaan Umum.

Pilih Langkah selanjutnya: Informasi tambahan

Subjek

Masukkan Memulihkan domain yang kedaluwarsa atau Memulihkan domain yang dihapus.

Deskripsi

Saat diminta, berikan informasi berikut:

- Domain yang ingin Anda pulihkan
- [ID akun 12 digit](#) dari AWS akun tempat domain terdaftar
- Konfirmasikan bahwa Anda setuju dengan harga tersebut untuk memulihkan domain.
Gunakan teks berikut:

“Saya setuju dengan harga \$_____ untuk memulihkan domain saya.”

Ganti bagian yang kosong dengan harga yang Anda temukan di langkah 2.

Metode kontak

Tentukan metode kontak dan masukkan nilai yang berlaku.

5. Pilih Kirim.
6. Ketika kami mengetahui apakah kami dapat memulihkan domain Anda, perwakilan AWS Support akan menghubungi Anda. Selain itu, jika kami dapat memulihkan domain Anda, domain tersebut akan muncul kembali di konsol. Tanggal kedaluwarsa tergantung apakah domain kedaluwarsa atau tidak sengaja dihapus:

Domain yang kedaluwarsa

Tanggal kedaluwarsa yang baru biasanya satu atau dua tahun (tergantung TLD) setelah

Memulihkan domain yang kedaluwarsa atau dihapus.
tanggal kedaluwarsa yang lama.

 Note

Tanggal kedaluwarsa baru tidak dihitung dari tanggal domain dipulihkan.

Domain itu secara tidak sengaja dihapus

Tanggal kedaluwarsa biasanya tidak berubah.

Mengganti zona yang di-hosting untuk domain yang terdaftar di Route 53

Jika Anda [menghapus zona yang di-hosting](#) untuk sebuah domain, Anda perlu membuat zona yang di-hosting lagi saat Anda siap untuk membuat domain tersedia di internet. Lakukan prosedur berikut.

Untuk mengganti zona yang di-hosting untuk domain

1. Membuat zona yang di-hosting publik. Untuk informasi selengkapnya, lihat [Membuat zona yang di-hosting publik](#).
2. Membuat catatan di zona yang di-hosting. Catatan menentukan bagaimana Anda ingin merutekan lalu lintas untuk domain (example.com) dan subdomain (acme.example.com, zenith.example.com). Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).
3. Memperbarui konfigurasi domain untuk menggunakan server nama untuk zona yang di-hosting baru. Untuk informasi selengkapnya, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

 Important

Saat Anda membuat zona yang di-hosting, Route 53 menetapkan empat server nama ke zona yang di-hosting. Jika Anda menghapus zona yang dihosting dan kemudian membuatnya, Route 53 menetapkan satu set lain dari empat server nama. Biasanya, tidak ada server nama untuk zona yang di-hosting baru yang cocok dengan server nama mana pun untuk zona yang di-hosting sebelumnya. Jika Anda tidak memperbarui konfigurasi domain untuk menggunakan server nama untuk zona yang di-hosting baru, domain tersebut akan tetap tidak tersedia di internet.

4. Jika Anda mengalami masalah saat mengganti zona yang dihosting untuk domain, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Mentransfer domain

Anda dapat mentransfer pendaftaran domain dari registrar lain ke Amazon Route 53, dari satu AWS akun ke akun lain, atau dari Route 53 ke registrar lain. Tidak ada biaya untuk mentransfer domain dari satu AWS akun ke akun lainnya.

Topik di bagian ini mencakup topik-topik berikut yang terkait dengan transfer domain:

1. [Pilih jenis transfer Anda](#)

- Pahami perbedaan antara mentransfer pendaftaran domain ke Route 53 versus menggunakan Route 53 hanya untuk hosting DNS.
- Pelajari opsi mana yang tepat untuk kebutuhan Anda berdasarkan tujuan Anda untuk manajemen domain dan hosting DNS.

2. [Daftar periksa pra-transfer](#)

- Selesaikan langkah-langkah persiapan penting sebelum mentransfer domain Anda ke Route 53 untuk menghindari kegagalan transfer umum.
- Verifikasi kelayakan domain, dapatkan kode otorisasi, dan siapkan pengaturan DNS Anda untuk proses transfer yang lancar.

3. [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#)

- Pelajari step-by-step prosedur untuk mentransfer domain dari registrar lain ke Route 53, termasuk prasyarat, kode otorisasi, dan memperbarui pengaturan DNS.
- Memahami bagaimana mentransfer domain memengaruhi tanggal kedaluwarsa dan pertimbangan untuk berbagai domain tingkat atas (). TLDs

4. [Masalah transfer umum](#)

- Mencegah masalah transfer umum dengan memahami persyaratan domain, proses otorisasi, dan pertimbangan waktu.
- Pelajari cara mengatasi masalah transfer dan apa yang harus dilakukan jika transfer Anda tertunda atau ditolak.

5. [Mentransfer domain dari Amazon Route 53 ke registrar lain](#)

- Memahami proses mentransfer domain dari Route 53 ke registrar lain, termasuk mendapatkan kode otorisasi, memperbarui pengaturan DNS, dan menanggapi email konfirmasi.
- Waspadaai pertimbangan saat mentransfer layanan DNS ke penyedia lain dan dampak potensial pada fitur khusus Route 53 seperti catatan alias dan kebijakan perutean.

6. [Mentransfer domain ke akun lain AWS](#)

- Cari tahu cara mentransfer domain dari satu AWS akun ke akun lainnya, termasuk peran dan izin yang diperlukan untuk memulai dan menerima transfer.
- Pelajari tentang langkah opsional untuk memigrasikan zona yang dihosting ke akun baru setelah transfer domain.

7. [Status transfer](#)

- Temukan cara melihat status permintaan transfer domain dan arti kode status yang berbeda selama proses transfer.

8. [Cara mentransfer domain ke Amazon Route 53 memengaruhi tanggal kedaluwarsa pendaftaran domain Anda](#)

- Cari tahu bagaimana mentransfer domain ke Route 53 dapat memengaruhi tanggal kedaluwarsa domain tersebut.

Dengan mengikuti informasi yang diberikan dalam topik yang tercantum di atas, Anda dapat secara efektif mentransfer domain ke dan dari Route 53, mengelola proses transfer, dan memastikan transisi yang lancar sambil mempertahankan konfigurasi dan perutean DNS yang tepat.

Pilih jenis transfer Route 53

Saat Anda ingin menggunakan Amazon Route 53 dengan domain Anda, Anda memiliki dua opsi. Memahami perbedaan akan membantu Anda memilih pendekatan yang tepat untuk kebutuhan Anda:

Transfer pendaftaran domain ke Route 53

Dengan opsi ini, Route 53 menjadi pendaftar domain Anda. Ini berarti Anda akan mengelola perpanjangan domain, informasi kontak, dan pengaturan DNS Anda melalui Route 53.

Pilih opsi ini jika Anda ingin:

- Konsolidasikan manajemen domain dan hosting DNS di satu tempat
- Manfaatkan fitur manajemen domain Route 53
- Sederhanakan penagihan dengan memiliki perpanjangan domain pada tagihan Anda AWS

Apa yang diharapkan:

- Waktu untuk menyelesaikan: 5-7 hari
- Prasyarat: Kode otorisasi dari registrar saat ini, buka kunci domain, verifikasi email pendaftar
- Siapa yang Anda bayar untuk pembaruan: Route 53

Langkah selanjutnya: Selesaikan [Daftar periksa pra-transfer untuk transfer domain](#) untuk mempersiapkan transfer.

Gunakan Route 53 hanya untuk hosting DNS

Dengan opsi ini, Anda menyimpan registrar domain Anda saat ini tetapi menggunakan Route 53 sebagai layanan DNS Anda.

Pilih opsi ini jika Anda ingin:

- Pertahankan hubungan registrar Anda yang ada
- Gunakan fitur DNS tingkat lanjut Route 53 tanpa mengubah pendaftar
- Memulai dengan cepat dengan prasyarat minimal

Apa yang diharapkan:

- Waktu untuk menyelesaikan: Hingga 2 hari (tergantung pada propagasi DNS)
- Prasyarat: Tidak ada
- Siapa yang Anda bayar untuk perpanjangan: Registrar Anda saat ini

Langkah selanjutnya: Buka [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#) untuk mengatur hosting DNS.

Important

Anda tidak perlu mentransfer pendaftaran domain Anda untuk menggunakan Route 53 sebagai layanan DNS Anda. Anda dapat menyimpan registrar yang ada dan menggunakan Route 53 hanya untuk hosting DNS.

Daftar Periksa pra-transfer untuk transfer domain

Sebelum Anda mulai mentransfer pendaftaran domain Anda ke Amazon Route 53, selesaikan pemeriksaan berikut untuk menghindari kegagalan transfer umum dan memastikan proses yang lancar.

Putuskan apa yang ingin Anda transfer

Pilih opsi yang sesuai dengan kebutuhan Anda:

Transfer pendaftaran domain ke Route 53

Registrar Anda menjadi Amazon Route 53. Anda membayar Route 53 untuk perpanjangan domain dan mengelola pengaturan domain melalui konsol Route 53.

Langkah selanjutnya: Lanjutkan dengan daftar Periksa ini, lalu ikuti. [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#)

Gunakan Route 53 hanya untuk hosting DNS

Simpan registrar Anda saat ini tetapi gunakan server nama Route 53 untuk resolusi DNS. Anda terus membayar registrar Anda saat ini untuk pembaruan.

Langkah selanjutnya: Lewati daftar Periksa ini dan ikuti. [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#)

Daftar Periksa prasyarat

Selesaikan semua hal berikut sebelum memulai transfer domain Anda.

Daftar Periksa pra-transfer (Lengkapi semua item)

1. ☐ Verifikasi akses email pendaftar

Konfirmasikan bahwa Anda dapat menerima email di alamat email pendaftar, karena akan menerima email otorisasi transfer domain.

 Important

Jika Anda tidak dapat mengakses alamat email pendaftar saat ini, perbarui alamat email untuk kontak pendaftar dengan pencatat Anda saat ini dan tunggu 60 hari sebelum mentransfer.

2. ☐ Buka kunci domain

Akses pengaturan domain registrar Anda saat ini dan nonaktifkan perlindungan “Domain Lock” atau “Transfer Lock”, jika diaktifkan.

 Note

Setelah menonaktifkan kunci, biarkan beberapa menit agar perubahan diterapkan sebelum memulai transfer Anda.

3. ☐ Dapatkan kode otorisasi

Minta kode otorisasi (kode autentikasi) dari registrar Anda saat ini dan jaga kerahasiaannya. Anda akan memasukkan kode ini di konsol Route 53 nanti dalam proses transfer.

4. ☐ Verifikasi usia dan kelayakan domain

Konfirmasikan domain Anda memenuhi persyaratan transfer ICANN:

- Domain harus berusia minimal 60 hari sejak pendaftaran awal.
- Jika pendaftaran domain kedaluwarsa dan dipulihkan, itu harus dipulihkan setidaknya 60 hari yang lalu.

 Tip

Aturan ICANN dapat memblokir transfer sementara jika rincian kontak pendaftar diperbarui baru-baru ini (misalnya, mengubah nama atau email Anda). Beberapa pendaftar mengizinkan Anda memilih keluar dari penangguhan ini — periksa dengan pencatat Anda saat ini jika Anda tidak yakin.

5. ☐ Siapkan metode pembayaran

Pastikan AWS akun Anda memiliki metode pembayaran yang valid. Saat Anda mentransfer domain ke Route 53, biaya transfer yang kami terapkan ke AWS akun Anda bervariasi menurut domain tingkat atas.

Untuk harga saat ini, lihat [Harga Route 53](#).

 Note

Anda tidak dapat menggunakan AWS kredit untuk membayar transfer domain. Route 53 membebaskan biaya transfer sebelum memulai proses dan memberikan pengembalian dana segera jika transfer gagal.

6. ☐ Nonaktifkan DNSSEC (jika diaktifkan)

Jika DNSSEC saat ini diaktifkan dengan registrar Anda saat ini, nonaktifkan sementara sebelum memulai transfer. Ini memastikan transfer dapat selesai tanpa masalah validasi DNS.

Mengapa ini penting:

Ketika Anda mentransfer domain, kunci DNSSEC (KSK/ZSK) dan catatan DS yang disimpan di registrar Anda saat ini tidak secara otomatis ditransfer ke Route 53. Jika Anda mengaktifkan kembali DNSSEC tanpa mengonfigurasi ulang kunci ini di Route 53, domain Anda mungkin gagal validasi DNS.

Pendekatan aman (disarankan):

1. Nonaktifkan DNSSEC di registrar Anda saat ini sebelum memulai transfer.
2. Selesaikan transfer domain dan buat zona host Route 53 Anda (jika belum dibuat).
3. Verifikasi bahwa semua catatan DNS diselesaikan dengan benar tanpa DNSSEC diaktifkan.
4. Konfigurasi DNSSEC di Route 53 menggunakan nilai baru KSK/ZSK zona host Anda.
5. Aktifkan kembali DNSSEC dengan menerbitkan catatan DS baru dengan registrar TLD Anda (sekarang Route 53).

 Tip

Jika Anda mentransfer domain Anda bersama dengan membuat zona host baru di Route 53, nonaktifkan DNSSEC sebelum mentransfer, lalu tunggu hingga pengaturan

zona yang dihosting diverifikasi dan resolusi DNS berfungsi dengan benar. Setelah dikonfirmasi, Anda dapat mengaktifkan DNSSEC dengan aman lagi dari konsol Route 53. Selalu verifikasi konfigurasi DNS Anda di Route 53 sebelum mengaktifkan kembali DNSSEC. Untuk informasi lebih lanjut tentang DNSSEC dengan Route 53, lihat.

[Mengonfigurasi DNSSEC untuk domain](#)

Opsional: Transfer layanan DNS terlebih dahulu

Pertimbangkan untuk mentransfer layanan DNS Anda ke Route 53 sebelum mentransfer pendaftaran domain. Pendekatan ini memberikan manfaat ini:

- Mengurangi risiko downtime situs web atau email selama transfer
- Memungkinkan Anda menguji fungsionalitas DNS Route 53 sebelum melakukan transfer penuh
- Menyediakan opsi fallback jika transfer domain mengalami masalah

Untuk mentransfer layanan DNS terlebih dahulu, lihat [Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda](#).

Langkah selanjutnya

Setelah menyelesaikan daftar periksa ini:

1. Ikuti proses step-by-step transfer di [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#).
2. Pantau email Anda untuk pesan otorisasi selama proses transfer.

Mentransfer pendaftaran untuk domain ke Amazon Route 53

Important

Selama transfer domain tingkat atas kode negara (ccTLDs) ke Route 53, kecuali untuk .cc dan .tv, pembaruan ke kontak pemilik diabaikan dan data kontak pemilik dari registri digunakan. Anda dapat memperbarui kontak pemilik setelah transfer selesai. Untuk informasi selengkapnya, lihat [Memperbarui informasi kontak dan kepemilikan domain](#).

Untuk mentransfer pendaftaran domain ke Amazon Route 53, ikuti prosedur dalam topik ini.

Ikhtisar proses transfer

Transfer domain melibatkan langkah-langkah kunci ini:

1. Daftar periksa pra-transfer lengkap

Verifikasi prasyarat untuk menghindari kegagalan transfer. Lihat [Daftar periksa pra-transfer untuk transfer domain](#).

2. Minta transfer di konsol Route 53

Masukkan nama domain dan kode otorisasi. Lihat [Langkah 5: Minta transfer](#).

3. Otorisasi melalui email (Diperlukan tindakan pelanggan)

Klik tautan otorisasi yang dikirim ke email pendaftar dalam waktu 5 hari. Lihat [Langkah 6: Klik tautan di email konfirmasi dan otorisasi](#).

4. Tunggu sampai selesai

Transfer selesai secara otomatis kecuali ditolak oleh registrar saat ini. Pantau status di konsol.

Poin kegagalan yang paling umum

Berikut ini adalah solusi untuk masalah umum:

- Email tidak diterima: Verifikasi email pendaftar dapat diakses dan periksa folder spam
- Domain terkunci: Buka kunci di registrar saat ini sebelum memulai transfer
- Kode autentikasi tidak valid: Minta kode otorisasi baru dari registrar saat ini
- Pelanggaran aturan 60 hari: Aturan ICANN 60 hari (jendela kelayakan). Transfer diblokir dalam waktu 60 hari sejak pendaftaran awal atau perubahan kontak pendaftar. Beberapa pendaftar mengizinkan opt-out sebelum perubahan—tanyakan registrar Anda saat ini jika ada.

Important

Jika Anda melewatkan satu langkah, domain Anda mungkin tidak tersedia di internet.

Perhatikan hal-hal berikut:

Menghubungi AWS Support

Jika mengalami masalah saat mentransfer domain, Anda dapat menghubungi AWS Support gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Tanggal kedaluwarsa

Untuk informasi tentang cara mentransfer domain memengaruhi tanggal kedaluwarsa saat ini, lihat [Cara mentransfer domain ke Amazon Route 53 memengaruhi tanggal kedaluwarsa pendaftaran domain Anda](#).

Biaya transfer

Saat Anda mentransfer domain ke Route 53, biaya transfer yang kami terapkan ke AWS akun Anda tergantung pada domain tingkat atas, seperti .com atau .org. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Anda tidak dapat menggunakan AWS kredit untuk membayar biaya, jika ada, untuk mentransfer domain ke Route 53.

Note

Route 53 mengenakan biaya untuk mentransfer domain Anda sebelum kami memulai proses transfer. Jika transfer gagal karena alasan tertentu, kami segera mengkreditkan akun Anda untuk biaya transfer.

Nama domain khusus dan premium

Registri TLD telah menetapkan harga khusus atau premium untuk beberapa nama domain. Anda tidak dapat mentransfer domain ke Route 53 jika domain tersebut memiliki harga khusus atau premium.

Kuota domain

Jumlah maksimum default domain per AWS akun adalah 20. Anda dapat [meminta kuota yang lebih tinggi](#). Untuk informasi selengkapnya, lihat [Kuota pada domain](#).

Batas server nama

Jumlah maksimum server nama per domain di Route 53 adalah 6.

Topik

- [Persyaratan transfer untuk domain tingkat atas](#)
- [Langkah 1: Konfirmasikan bahwa Amazon Route 53 mendukung domain tingkat atas](#)
- [Langkah 2 \(Opsional\): Transfer layanan DNS Anda ke Amazon Route 53 atau penyedia layanan DNS lainnya](#)
- [Langkah 3: Ubah pengaturan dengan registrar saat ini](#)
- [Langkah 4: Dapatkan nama server nama Anda](#)
- [Langkah 5: Minta transfer](#)
- [Langkah 6: Klik tautan di email konfirmasi dan otorisasi](#)
- [Langkah 7: Perbarui konfigurasi domain](#)

Persyaratan transfer untuk domain tingkat atas

Sebagian besar pendaftar domain memberlakukan persyaratan untuk mentransfer domain ke registrar lain. Tujuan utama dari persyaratan ini adalah untuk mencegah pemilik domain palsu agar tidak berulang kali mentransfer domain ke registrar yang berbeda. Persyaratan bervariasi, tetapi persyaratan berikut adalah khusus:

- Anda harus telah mendaftarkan domain dengan registrar saat ini atau mentransfer pendaftaran domain ke registrar saat ini setidaknya 60 hari yang lalu.
- Jika pendaftaran untuk nama domain kedaluwarsa dan harus dipulihkan, pendaftaran harus dipulihkan setidaknya 60 hari yang lalu.
- Domain tidak boleh memiliki salah satu dari kode status nama domain berikut:
 - `clientTransferProhibited`
 - `pendingDelete`
 - `pendingTransfer`
 - `redemptionPeriod`
 - `serverTransferProhibited`
- Registri untuk beberapa domain tingkat atas tidak mengizinkan transfer hingga perubahan selesai, seperti perubahan pada pemilik domain.

Untuk daftar kode status nama domain saat ini dan penjelasan tentang arti setiap kode, kunjungi [situs web untuk ICANN](#), dan cari kode status EPP. (Penelusuran di situs web ICANN; penelusuran web terkadang mengembalikan versi dokumen yang lama.)

 Note

ICANN adalah organisasi yang menetapkan kebijakan yang mengatur pendaftaran dan transfer nama domain.

Anda juga dapat mencari nama domain Anda di [situs web untuk Whois](#) untuk melihat kode status dan informasi lain untuk domain Anda.

Langkah 1: Konfirmasikan bahwa Amazon Route 53 mendukung domain tingkat atas

Lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#). Jika domain tingkat atas untuk domain yang ingin Anda transfer ada dalam daftar, Anda dapat mentransfer domain ke Amazon Route 53.

Jika TLD tidak ada dalam daftar, saat ini Anda tidak dapat mentransfer pendaftaran domain ke Route 53. Kami sesekali menambahkan lebih banyak TLDs ke daftar, jadi periksa kembali untuk melihat apakah kami telah menambahkan dukungan untuk domain Anda.

Langkah 2 (Opsional): Transfer layanan DNS Anda ke Amazon Route 53 atau penyedia layanan DNS lainnya

Mengapa mentransfer DNS terlebih dahulu?

Beberapa registrar menyediakan layanan DNS gratis yang mungkin dinonaktifkan segera setelah mereka menerima permintaan dari Route 53 untuk mentransfer pendaftaran domain. Jika Anda ingin Route 53 menyediakan layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Langkah 3: Ubah pengaturan dengan registrar saat ini

Dengan menggunakan metode yang disediakan oleh registrar Anda saat ini, lakukan setiap hal berikut untuk setiap domain yang ingin Anda transfer.

- [Confirm that the email for the registrant contact for your domain is up to date](#)
- [Unlock the domain so it can be transferred](#)

- [Confirm that the domain status allows you to transfer the domain](#)
- [Disable DNSSEC for the domain](#)
- [Get an authorization code](#)
- [Renew your domain registration before you transfer the domain \(selected geographic TLDs\)](#)

Konfirmasikan bahwa email untuk kontak pendaftar untuk domain Anda adalah yang terbaru

Kami akan mengirimkan email ke alamat email tersebut untuk meminta otorisasi transfer. Anda perlu mengeklik tautan di email untuk mengotorisasi transfer. Jika Anda tidak mengklik tautan, kami harus membatalkan transfer.

 Important

Kontak yang Anda cantumkan sebagai pendaftar akan memiliki hak tertentu sebagai Pemegang Nama Terdaftar untuk nama domain, berdasarkan [Kebijakan Transfer ICANN](#). Sebagian besar domain akan dihapus setelah penutupan Anda Akun AWS (untuk informasi lebih lanjut, lihat [AWS Akun saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53](#)), namun jika domain tetap berada di akun tertutup, kontak yang Anda daftarkan sebagai pendaftar mungkin memiliki kemampuan untuk meminta transfer nama domain ke pencatat eksternal. Oleh karena itu, kontak pendaftar yang Anda cantumkan sebaiknya adalah diri Anda sendiri atau orang lain yang Anda percayai untuk bertindak secara bertanggung jawab.

Buka kunci domain agar dapat ditransfer

ICANN, badan pengelola untuk pendaftaran domain mengharuskan Anda membuka kunci domain sebelum mentransfernya.

Konfirmasikan bahwa status domain memungkinkan Anda mentransfer domain

Untuk informasi selengkapnya, lihat [Persyaratan transfer untuk domain tingkat atas](#).

Nonaktifkan DNSSEC untuk domain

Jika Anda menggunakan DNSSEC dengan domain dan Anda mentransfer pendaftaran domain ke Route 53, Anda harus menonaktifkan DNSSEC di registrar sebelumnya terlebih dahulu. Kemudian, setelah Anda mentransfer pendaftaran domain, lakukan langkah-langkah untuk menyiapkan DNSSEC untuk domain di Route 53. Route 53 mendukung DNSSEC untuk

pendaftaran domain dan untuk penandatanganan DNSSEC. Untuk informasi selengkapnya, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

 Important

Jika Anda mentransfer pendaftaran domain ke Route 53 saat DNSSEC dikonfigurasi, kunci publik DNSSEC juga akan ditransfer. Jika Anda mentransfer layanan DNS ke penyedia yang tidak mendukung DNSSEC, resolusi DNS akan gagal sewaktu-waktu hingga Anda menghapus kunci DNSSEC dari domain. Untuk informasi selengkapnya, lihat [Menghapus kunci publik untuk domain](#).

Dapatkan kode otorisasi

Kode otorisasi dari registrar saat ini memberi wewenang kepada kami untuk meminta agar pendaftaran domain ditransfer ke Route 53. Anda akan memasukkan kode ini di konsol Route 53 nanti dalam prosesnya.

Beberapa domain tingkat atas memiliki persyaratan tambahan:

Domain .co.za

Anda tidak perlu mendapatkan kode otorisasi untuk mentransfer domain .co.za ke Route 53.

Domain .uk, .co.uk, .me.uk, dan .org.uk

Jika Anda mentransfer domain .uk, .co.uk, .me.uk, atau .org.uk ke Route 53, Anda tidak perlu mendapatkan kode otorisasi. Sebaliknya, gunakan metode yang disediakan oleh registrar domain Anda saat ini untuk memperbarui nilai tanda IPS untuk domain GANDI, semua huruf besar. (Tanda IPS diperlukan oleh Nominet, registri untuk nama domain .uk.) Jika registrar Anda tidak menyediakan cara untuk mengubah nilai tanda IPS, [Hubungi Nominet](#).

Perhatikan hal berikut tentang mengubah tanda IPS:

Anda harus meminta transfer dalam waktu lima hari

Jika Anda tidak meminta transfer dalam waktu lima hari setelah Anda mengubah tanda IPS, tanda akan berubah kembali ke nilai sebelumnya. Anda harus mengubah nilai tanda IPS lagi, atau permintaan transfer akan gagal.

Melihat tanda IPS dalam kueri WHOIS

Perubahan untuk tanda IPS tidak muncul dalam permintaan WHOIS sampai setelah transfer ke Route 53 telah selesai.

Email dari Gandi

Anda mungkin menerima email dari rekan registrar kami, Gandi, tentang proses transfer. Jika Anda menerima email dari Gandi (transfer-auth@gandi.net) tentang mentransfer domain Anda, abaikan instruksi di email karena tidak relevan dengan domain.uk, .co.uk, .me.uk, atau.org.uk. Ikuti petunjuk dalam topik ini sebagai gantinya.

Perbarui pendaftaran domain Anda sebelum Anda mentransfer domain (geografis TLDs yang dipilih)

Untuk sebagian besar TLDs, ketika Anda mentransfer domain, pendaftaran secara otomatis diperpanjang satu tahun. Namun, untuk beberapa geografis TLDs, pendaftaran tidak diperpanjang ketika Anda mentransfer domain. Jika Anda mentransfer domain ke Route 53 yang memiliki salah satunya TLDs, kami sarankan Anda memperbarui pendaftaran domain sebelum mentransfer domain, terutama jika tanggal kedaluwarsa sudah dekat.



Important

Jika Anda tidak memperbarui domain sebelum mentransfernya, pendaftaran dapat kedaluwarsa sebelum transfer selesai. Jika ini terjadi, domain menjadi tidak tersedia di internet, dan nama domain dapat tersedia untuk dibeli orang lain.

Pendaftaran tidak diperpanjang secara otomatis saat Anda mentransfer domain berikut ke registrar lain:

- .ch (Swiss)
- .cl (Chili)
- .co.uk (Inggris Raya)
- .co.za (Afrika Selatan)
- .com.au (Australia)
- .cz (Republik Ceko)
- .es (Spanyol)
- .fi (Finlandia)
- .im (Pulau Man)
- .jp (Jepang)
- .me.uk (Inggris Raya)

- .net.au (Australia)
- .org.uk (Inggris Raya)
- .se (Swedia)
- .uk (Inggris Raya)

Langkah 4: Dapatkan nama server nama Anda

Jika Anda menggunakan Amazon Route 53 sebagai layanan DNS Anda atau Anda terus menggunakan layanan DNS yang ada, kami akan mendapatkan nama server nama untuk Anda secara otomatis nanti dalam prosesnya. Loncat ke [Langkah 5: Minta transfer](#).

Jika Anda ingin mengubah layanan DNS ke penyedia selain Route 53 pada saat yang sama saat Anda mentransfer domain ke Route 53, gunakan prosedur yang disediakan oleh penyedia layanan DNS untuk mendapatkan nama server nama untuk setiap domain yang ingin Anda transfer.

Important

Jika pencatat domain Anda juga merupakan penyedia layanan DNS untuk domain tersebut, transfer layanan DNS Anda ke Route 53 atau penyedia layanan DNS lainnya sebelum Anda melanjutkan proses untuk mentransfer pendaftaran domain.

Jika Anda mentransfer layanan DNS pada saat yang sama dengan Anda mentransfer pendaftaran domain, situs web, email, dan aplikasi web Anda yang terkait dengan domain mungkin menjadi tidak tersedia. Untuk informasi selengkapnya, lihat [Langkah 2 \(Opsional\): Transfer layanan DNS Anda ke Amazon Route 53 atau penyedia layanan DNS lainnya](#).

Langkah 5: Minta transfer

Untuk mentransfer pendaftaran domain dari registrar saat ini ke Amazon Route 53, gunakan konsol Route 53 untuk meminta transfer. Route 53 menangani komunikasi dengan pencatat domain saat ini.

Anda dapat menggunakan konsol untuk mentransfer hingga lima domain.

Prosedur yang Anda gunakan tergantung pada apakah Anda ingin mentransfer satu domain atau hingga lima domain:

- [Untuk mentransfer pendaftaran domain dari satu domain ke Route 53](#)
- [Untuk mentransfer pendaftaran domain ke Route 53 hingga lima domain](#)

Gunakan proses Transfer domain ke akun Anda untuk mentransfer satu domain ke akun Anda.

Untuk mentransfer pendaftaran domain dari satu domain ke Route 53

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pada halaman Domain Terdaftar, pilih Domain tunggal dari menu tarik-turun Transfer di.
4. Pada halaman Transfer domain ke akun Anda, di bagian Periksa transfer domain, masukkan nama domain yang ingin Anda transfer pendaftaran ke Route 53, dan pilih Periksa.
5. Jika pendaftaran domain tersedia untuk transfer, verifikasi bahwa Anda telah menyelesaikan persyaratan transfer untuk domain tingkat atas, dan pilih Berikutnya.

Jika pendaftaran domain tidak tersedia untuk transfer, konsol Route 53 mencantumkan alasannya. Hubungi pencatat Anda untuk informasi tentang cara mengatasi masalah yang mencegah Anda mentransfer pendaftaran.

6. Pada halaman layanan DNS, tinjau informasi tentang server nama, dan pilih Berikutnya.
7. Jika diminta, masukkan kode otorisasi atau tag IPS yang Anda dapatkan dari registrar Anda saat ini. [Langkah 3: Ubah pengaturan dengan registrar saat ini](#)

 Note

Anda tidak perlu memasukkan kode otorisasi untuk mentransfer domain.co.za, .uk, .co.uk, .me.uk, atau .org.uk ke Route 53.

Pilih Berikutnya.

8. Pada halaman opsi harga Domain, pilih jumlah tahun yang Anda inginkan untuk mendaftarkan domain yang Anda transfer dan apakah Anda ingin kami memperbarui pendaftaran domain Anda secara otomatis sebelum tanggal kedaluwarsa.

 Note

Pendaftaran dan perpanjangan nama domain tidak bisa mendapatkan pengembalian dana. Jika Anda mengaktifkan perpanjangan domain otomatis dan Anda memutuskan bahwa Anda tidak menginginkan nama domain setelah kami memperbarui pendaftaran, Anda tidak bisa mendapatkan pengembalian dana untuk biaya perpanjangan.

Pilih Berikutnya.

9. Pada halaman Informasi kontak, masukkan informasi kontak untuk pendaftar domain, admin, teknis, dan kontak penagihan. Nilai yang Anda masukkan di sini diterapkan ke semua domain yang Anda daftarkan. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat mendaftar atau mentransfer domain](#).

Perhatikan pertimbangan berikut:

Nama Depan dan Nama Belakang

Untuk Nama Depan dan Nama Belakang, kami sarankan Anda mencantumkan nama tersebut pada ID resmi Anda. Untuk beberapa perubahan pada pengaturan domain, beberapa registri domain mengharuskan Anda memberikan bukti identitas. Nama di ID Anda harus sesuai dengan nama kontak pendaftar untuk domain tersebut.

Kontak yang berbeda

Secara default, kami menggunakan informasi yang sama untuk ketiga kontak tersebut. Jika Anda ingin memasukkan informasi yang berbeda untuk satu atau beberapa kontak, ubah nilai Sama seperti kontak pendaftar sakelar sakelar ke posisi mati.



Note

Untuk domain.it, pendaftar dan kontak admin harus sama.

Informasi tambahan yang diperlukan

Untuk beberapa domain tingkat atas (TLDs), kami diminta untuk mengumpulkan informasi tambahan. Untuk ini TLDs, masukkan nilai yang berlaku setelah bidang Kode Postal/Pos.

Perlindungan privasi

Pilih apakah Anda ingin menyembunyikan informasi kontak Anda dari kueri WHOIS.



Note

Anda harus menentukan pengaturan privasi yang sama untuk admin, pendaftar, dan kontak teknis.

Untuk informasi selengkapnya, lihat topik berikut:

- [Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain](#)
- [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

 Note

Untuk mengaktifkan perlindungan privasi untuk domain.uk, .co.uk, .me.uk, dan .org.uk, Anda harus membuka kasus dukungan dan meminta perlindungan privasi.

Pilih Berikutnya.

10. Pada halaman Ulasan, tinjau informasi yang Anda masukkan, dan perbaiki secara opsional. Baca persyaratan layanan, dan pilih kotak centang untuk mengonfirmasi bahwa Anda telah membaca persyaratan layanan.

Pilih Kirim permintaan.

11. Di panel navigasi, pilih Domain dan kemudian Permintaan.

Di halaman ini, Anda dapat melihat status domain dan juga jika Anda perlu menanggapi email verifikasi kontak pendaftar. Anda juga dapat memilih untuk mengirim ulang email verifikasi.

Jika Anda menentukan alamat email untuk kontak pendaftar yang belum pernah digunakan untuk mendaftarkan domain dengan Route 53, beberapa pendaftar TLD mengharuskan Anda untuk memverifikasi bahwa alamat tersebut valid.

Kami mengirim email verifikasi dari salah satu alamat email berikut:

- `noreply@registrar.amazon` - untuk TLDs didaftarkan oleh Amazon Registrar.
- `noreply@domainnameverification.net` atau `noreply@emailverification.info` — untuk TLDs didaftarkan oleh rekanan registrar kami, Gandi. Untuk menentukan registrar TLD Anda, lihat [Menemukan registrar Anda](#).

 Important

Kontak pendaftar harus mengikuti petunjuk dalam email untuk memverifikasi bahwa email telah diterima, atau kami harus menangguhkan domain seperti yang disyaratkan oleh ICANN. Jika ditangguhkan, domain tersebut tidak dapat diakses di internet.

- a. Saat Anda menerima email verifikasi, pilih tautan di email yang memverifikasi bahwa alamat email tersebut valid. Jika Anda tidak segera menerima email tersebut, periksa folder email sampah Anda.
 - b. Kembali ke halaman Permintaan. Jika status tidak diperbarui secara otomatis dan muncul pesan email-address is verified (alamat email telah diverifikasi), pilih Refresh status (Segarkan status).
12. Ketika transfer domain selesai, langkah selanjutnya tergantung pada apakah Anda ingin menggunakan Route 53 atau layanan DNS lain sebagai layanan DNS untuk domain:
- Route 53 — Di zona host yang dibuat Route 53 saat Anda mendaftarkan domain, buat catatan untuk memberi tahu Route 53 bagaimana Anda ingin merutekan lalu lintas untuk domain dan subdomain.

Misalnya, ketika seseorang memasukkan nama domain Anda di browser dan kueri tersebut diteruskan ke Route 53, apakah Anda ingin Route 53 menanggapi kueri dengan alamat IP server web di pusat data Anda atau dengan nama penyeimbang beban Elastic Load Balancing?

Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).

 Important

Jika Anda membuat rekaman di zona yang di-hosting selain yang dibuat oleh Route 53 secara otomatis, Anda harus memperbarui server nama domain untuk menggunakan server nama untuk zona baru yang di-hosting.

- Layanan DNS lainnya – Konfigurasi domain baru Anda untuk merutekan kueri DNS ke layanan DNS lainnya. Lakukan prosedur [Memperbarui server nama untuk menggunakan registrar lain](#).

Gunakan prosedur berikut untuk mentransfer hingga lima domain ke akun Anda.

Untuk mentransfer pendaftaran domain ke Route 53 hingga lima domain

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pada halaman Domain terdaftar, pilih Beberapa domain dari menu tarik-turun Transfer di.
4. Pada halaman Transfer beberapa domain ke akun Anda, masukkan hingga lima domain yang ingin Anda transfer, dan kode otorisasi mereka, jika diperlukan, per baris, dan pilih Periksa.
5. Jika pendaftaran domain tersedia untuk transfer, itu tercantum dalam daftar ketersediaan Domain yang tersedia. Pilih kotak centang di samping setiap domain yang ingin Anda transfer pendaftarannya, verifikasi bahwa Anda telah menyelesaikan persyaratan transfer untuk domain tingkat atas, dan pilih Berikutnya.

Jika pendaftaran domain tidak tersedia untuk transfer, konsol Route 53 mencantumkan alasannya. Hubungi pencatat Anda untuk informasi tentang cara mengatasi masalah yang mencegah Anda mentransfer pendaftaran.

6. Pada halaman layanan DNS, tinjau informasi tentang server nama, dan pilih Berikutnya.

 Note

Pendaftaran dan perpanjangan nama domain tidak dapat dikembalikan. Jika Anda mengaktifkan perpanjangan domain otomatis dan Anda memutuskan bahwa Anda tidak menginginkan nama domain setelah kami memperbarui pendaftaran, Anda tidak bisa mendapatkan pengembalian dana untuk biaya perpanjangan.

7. Pada halaman Informasi kontak, masukkan informasi kontak untuk pendaftar domain, admin, dan kontak teknis. Nilai yang Anda masukkan di sini diterapkan ke semua domain yang Anda transfer.

 Important

Kami menyarankan Anda menentukan nilai berikut untuk kontak pendaftar (pemilik domain):

- Nama depan dan belakang: Kami menyarankan agar Anda menentukan nama yang muncul di ID resmi Anda. Untuk beberapa perubahan pada pengaturan domain,

beberapa pendaftar domain mengharuskan Anda memberikan bukti identitas. Nama di ID Anda harus sesuai dengan nama kontak pendaftar untuk domain tersebut.

- **Detail kontak:** Selama transfer domain, kami menyarankan Anda menentukan nilai yang sama seperti yang ditentukan dengan registrar saat ini. Saat Anda mengubah detail kontak untuk kontak pendaftar, Anda mengubah pemilik domain, dan beberapa pendaftar TLD tidak mengizinkan Anda mengubah pemilik domain selama transfer domain. Jika Anda mengubah detail kontak untuk kontak pendaftar, transfer mungkin gagal. Anda dapat mengubah detail kontak untuk kontak pendaftar setelah Anda mentransfer domain.

Secara default, kami menggunakan informasi yang sama untuk ketiga kontak tersebut. Jika Anda ingin memasukkan informasi yang berbeda untuk satu atau beberapa kontak, tetapkan nilai Sama seperti kontak pendaftar ke posisi mati.

 Note

Untuk domain.it, pendaftar dan kontak admin harus sama.

Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat mendaftar atau mentransfer domain](#).

8. Untuk beberapa orang TLDs, kami diminta untuk mengumpulkan informasi tambahan. Untuk iniTLDs, masukkan nilai yang berlaku setelah bidang Kode Postal/Pos.
9. Jika nilai Jenis Kontak adalah Orang, pilih apakah Anda ingin menyembunyikan informasi kontak dari kueri WHOIS. Untuk informasi selengkapnya, lihat [Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain](#).
10. Pilih Kirim.
11. Tinjau informasi yang Anda masukkan, baca syarat layanan, dan pilih kotak centang untuk mengonfirmasi bahwa Anda telah membaca syarat layanan.
12. Pilih Kirim permintaan.

Kami mengonfirmasi bahwa domain memenuhi syarat untuk ditransfer, dan kami mengirim email ke kontak pendaftar untuk domain untuk meminta otorisasi untuk mentransfer domain.

13. Di panel navigasi, pilih Domain dan kemudian Permintaan.

Pada halaman ini Anda dapat melihat status domain dan juga jika Anda perlu menanggapi email verifikasi kontak pendaftar. Anda juga dapat memilih untuk mengirim ulang email verifikasi.

Jika Anda menentukan alamat email untuk kontak pendaftar yang belum pernah digunakan untuk mendaftarkan domain dengan Route 53, beberapa pendaftar TLD mengharuskan Anda untuk memverifikasi bahwa alamat tersebut valid.

Kami mengirim email verifikasi dari salah satu alamat email berikut:

- `noreply@registrar.amazon` - untuk TLDs didaftarkan oleh Amazon Registrar.
- `noreply@domainnameverification.net` atau `noreply@emailverification.info` — untuk TLDs didaftarkan oleh rekanan registrar kami, Gandi. Untuk menentukan registrar TLD Anda, lihat [Menemukan registrar Anda](#).

 Important

Kontak pendaftar harus mengikuti petunjuk dalam email untuk memverifikasi bahwa email telah diterima, atau kami harus menangguhkan domain seperti yang disyaratkan oleh ICANN. Jika ditangguhkan, domain tersebut tidak dapat diakses di internet.

- a. Saat Anda menerima email verifikasi, pilih tautan di email yang memverifikasi bahwa alamat email tersebut valid. Jika Anda tidak segera menerima email tersebut, periksa folder email sampah Anda.
 - b. Kembali ke halaman Permintaan. Jika status tidak diperbarui secara otomatis dan muncul pesan `email-address is verified` (alamat email telah diverifikasi), pilih Refresh status (Segarkan status).
14. Ketika transfer domain selesai, langkah selanjutnya tergantung pada apakah Anda ingin menggunakan Route 53 atau layanan DNS lain sebagai layanan DNS untuk domain:
- Route 53 — Di zona host yang dibuat Route 53 saat Anda mendaftarkan domain, buat catatan untuk memberi tahu Route 53 bagaimana Anda ingin merutekan lalu lintas untuk domain dan subdomain.

Misalnya, ketika seseorang memasukkan nama domain Anda di peramban dan kueri itu diteruskan ke Route 53, apakah Anda ingin Route 53 merespons kueri dengan alamat IP server web di pusat data Anda atau dengan nama penyeimbang beban ELB?

Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).

 Important

Jika Anda membuat rekaman di zona yang di-hosting selain yang dibuat oleh Route 53 secara otomatis, Anda harus memperbarui server nama domain untuk menggunakan server nama untuk zona baru yang di-hosting.

- Layanan DNS lainnya – Konfigurasi domain baru Anda untuk merutekan kueri DNS ke layanan DNS lainnya. Lakukan prosedur [Memperbarui server nama untuk menggunakan registrar lain](#).

Langkah 6: Klik tautan di email konfirmasi dan otorisasi

Segera setelah Anda meminta transfer, kami mungkin mengirim satu atau beberapa email ke kontak pendaftar untuk domain tersebut:

Email untuk mengonfirmasi bahwa kontak pendaftar dapat dijangkau

Jika Anda belum pernah mendaftarkan domain dengan Route 53 atau mentransfer domain ke Route 53, kami akan mengirimkan email yang meminta Anda untuk mengonfirmasi bahwa alamat email tersebut valid. Kami menyimpan informasi ini sehingga kami tidak perlu mengirim email konfirmasi ini lagi.

Email untuk mendapatkan otorisasi untuk mentransfer domain

Untuk beberapa orang TLDs, Anda perlu menanggapi email untuk mengotorisasi transfer domain. Generik TLDs seperti .com, .net, dan .org

Otorisasi tidak diperlukan untuk domain yang memiliki [TLD umum](#), seperti .com, .net, atau .org.

Geografis TLDs seperti .co.uk dan .jp

Untuk domain yang memiliki [TLD geografis](#), kami diminta untuk mendapatkan otorisasi Anda untuk mentransfer domain. Jika Anda mentransfer 10 domain, kami harus mengirim Anda 10 email, dan Anda harus mengklik tautan otorisasi di masing-masing domain.

Semua email masuk ke kontak pendaftar untuk domain:

- Jika Anda adalah kontak pendaftar untuk domain tersebut, ikuti petunjuk dalam email untuk mengotorisasi transfer.
- Jika orang lain adalah kontak pendaftar, minta orang tersebut untuk mengikuti petunjuk dalam email untuk mengotorisasi transfer.

Important

Jika Anda mentransfer domain yang memiliki TLD geografis, kami menunggu hingga lima hari hingga kontak pendaftar mengotorisasi transfer tersebut. Jika kontak pendaftar tidak merespons dalam lima hari, kami membatalkan operasi transfer dan mengirim email ke kontak pendaftar tentang pembatalan tersebut.

Topik

- [Email otorisasi untuk pemilik atau alamat email baru](#)
- [Alamat email asal email otorisasi](#)
- [Persetujuan dari registrar saat ini](#)
- [Apa yang terjadi selanjutnya](#)

Email otorisasi untuk pemilik atau alamat email baru

Jika Anda mengubah nilai berikut, kami akan mengirimkan email terpisah yang meminta otorisasi Anda:

Pemilik domain

Jika Anda mengubah pemilik domain, seperti yang dijelaskan di [Apa yang memicu perubahan kepemilikan domain?](#), kami mengirim email ke kontak pendaftar untuk domain tersebut.

Alamat email untuk kontak pendaftar (hanya untuk beberapa TLDs)

Bagi sebagian orang TLDs, jika Anda mengubah alamat email untuk kontak pendaftar, kami mengirim email ke alamat email lama dan baru untuk kontak pendaftar. Seseorang di kedua alamat email harus mengikuti petunjuk dalam email untuk mengotorisasi perubahan.

Untuk perubahan pada pemilik domain atau alamat email untuk kontak pendaftar, jika kami tidak menerima otorisasi untuk perubahan dalam waktu 3-15 hari, tergantung pada domain tingkat atas, kami harus membatalkan permintaan seperti yang dipersyaratkan oleh ICANN.

Alamat email asal email otorisasi

Semua email berasal dari salah satu alamat email berikut.

TLDs	Alamat email asal email otorisasi
.com.au dan .net.au	no-reply@ispapi.net Email berisi tautan ke http://transfers.ispapi.net .
.fr	nic@nic.fr, jika Anda mengubah kontak pendaftar untuk nama domain.fr secara bersamaan saat Anda mentransfer domain. (Email dikirim ke kontak pendaftar saat ini dan kontak pendaftar baru.)
Semua yang lain	Salah satu alamat email berikut: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

Untuk menentukan registrar TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Persetujuan dari registrar saat ini

Jika kontak pendaftar mengotorisasi transfer, kami mulai bekerja dengan registrar Anda saat ini untuk mentransfer domain Anda. Langkah ini mungkin memerlukan waktu hingga sepuluh hari, bergantung pada TLD untuk domain Anda:

- [Domain tingkat atas generik](#) – memakan waktu hingga tujuh hari

- [Domain tingkat atas geografis](#) (juga dikenal sebagai domain tingkat atas kode negara) – membutuhkan waktu hingga sepuluh hari

Jika registrar Anda saat ini tidak membalas permintaan transfer kami, yang biasa terjadi di antara registrar, transfer terjadi secara otomatis. Jika registrar Anda saat ini menolak permintaan transfer, kami mengirimkan pemberitahuan email ke kontak pendaftar saat ini. Pendaftar harus menghubungi registrar saat ini dan menyelesaikan masalah terkait transfer.

Apa yang terjadi selanjutnya

Ketika transfer domain Anda telah disetujui, kami akan mengirim email lain ke kontak pendaftar. Untuk informasi selengkapnya tentang prosesnya, lihat [Melihat status transfer domain](#).

Kami menagih AWS akun Anda untuk transfer domain segera setelah transfer selesai. Untuk daftar biaya oleh TLD, lihat [Harga Amazon Route 53 untuk Pendaftaran Domain](#).

Note

Ini adalah tagihan satu kali, sehingga tagihan tidak muncul di metrik CloudWatch penagihan Anda. Untuk informasi selengkapnya tentang CloudWatch metrik, lihat [Menggunakan CloudWatch metrik Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Langkah 7: Perbarui konfigurasi domain

Setelah transfer selesai, Anda dapat mengubah pengaturan berikut secara opsional:

Kunci transfer

Untuk mentransfer domain ke Route 53, Anda harus menonaktifkan kunci transfer. Jika Anda ingin mengaktifkan kembali kunci untuk mencegah transfer yang tidak sah, lihat [Mengunci domain untuk mencegah transfer tidak sah ke registrar lain](#).

Perpanjangan otomatis

Kami mengonfigurasi domain yang ditransfer untuk diperpanjang secara otomatis saat mendekati tanggal kedaluwarsa. Untuk informasi tentang cara mengubah pengaturan ini, lihat [Mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain](#).

Periode pendaftaran diperpanjang

Secara default, Route 53 memperbarui domain setiap tahun. Jika Anda ingin mendaftarkan domain untuk periode yang lebih lama, lihat [Memperpanjang masa pendaftaran untuk domain](#).

DNSSEC

Untuk informasi tentang konfigurasi DNSSEC untuk domain, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Mencegah masalah transfer Route 53 yang umum

Jika Anda mengalami masalah saat transfer domain sedang berlangsung, berikut adalah masalah yang paling umum dan cara mengatasinya:

Note

Jika transfer Anda gagal, lihat [Gagal mentransfer domain saya ke Amazon Route 53](#) pemecahan masalah pasca-kegagalan.

Anda tidak menerima email otorisasi

Jika Anda tidak menerima email otorisasi dari Route 53, berikut adalah penyebab dan solusi paling umum:

- Periksa folder spam Anda - Email otorisasi terkadang difilter oleh penyedia email.
- Verifikasi alamat email Anda - Konfirmasikan bahwa alamat email pendaftar di informasi kontak domain Anda terkini dan dapat diakses.
- Perbarui informasi kontak Anda - Jika alamat email sudah usang, perbarui dengan registrar Anda saat ini sebelum memulai transfer.
- Kirim ulang email otorisasi - Di konsol Route 53, klik “Kirim ulang email otorisasi” untuk domain dalam status transfer.

Anda mendapatkan kesalahan “kode otorisasi tidak valid”

Jika Anda menerima kesalahan “kode otorisasi tidak valid”, coba solusi ini:

- Periksa ulang kode - Kode otorisasi peka huruf besar/kecil. Salin dan tempel kode langsung dari antarmuka registrar Anda untuk menghindari kesalahan pengetikan.

- Periksa apakah kode telah kedaluwarsa - Kode otorisasi dapat kedaluwarsa antara 5-30 hari tergantung pada registrar Anda saat ini. Minta kode baru jika kode Anda telah kedaluwarsa.
- Hapus spasi ekstra - Pastikan tidak ada spasi depan atau belakang saat Anda memasukkan kode.
- Dapatkan kode otorisasi baru - Jika kode terus gagal, minta kode otorisasi baru dari registrar Anda saat ini.

Domain Anda dikunci di registrar saat ini

Transfer domain dapat gagal ketika registrar Anda saat ini mengaktifkan kunci transfer (juga dikenal sebagai “Kunci Domain” atau “Transfer Klien Dilarang”). Ini adalah pengaturan keamanan umum yang mencegah transfer yang tidak sah.

Untuk menyelesaikan masalah ini:

- Buka kunci domain Anda - Masuk ke panel kontrol registrar Anda saat ini dan nonaktifkan kunci transfer domain.
- Verifikasi kunci dihapus - Anda dapat menggunakan alat pencarian WHOIS publik apa pun untuk mengonfirmasi bahwa status domain menunjukkan “OK” alih-alih “clientTransferProhibited.”
- Dapatkan bantuan dari registrar Anda - Jika Anda tidak melihat opsi untuk membuka kunci domain Anda, hubungi tim dukungan registrar Anda saat ini. Mereka dapat membantu Anda melepas kunci.

Domain Anda tidak memenuhi syarat untuk ditransfer

Jika transfer domain Anda ditolak karena masalah kelayakan, periksa hal berikut:

- Verifikasi usia domain - Domain Anda harus berusia minimal 60 hari sejak pendaftaran atau transfer terakhir.
- Periksa dukungan TLD - Konfirmasikan bahwa Route 53 mendukung domain tingkat atas (TLD) domain Anda. Lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#) untuk didukung TLDs.
- Tinjau status domain - Domain dengan kode status tertentu (seperti “PendingTransfer” atau “RedemptionPeriod”) tidak dapat ditransfer.
- Periksa tanggal kedaluwarsa - Domain yang kedaluwarsa atau dalam waktu 15 hari setelah kedaluwarsa mungkin tidak dapat dipindahtangankan.
- Selesaikan masalah penagihan - Pastikan semua biaya terutang dengan registrar Anda saat ini dibayar.

Transfer Anda memakan waktu lebih lama dari yang diharapkan

Jika transfer Anda tampaknya tertunda, inilah yang harus Anda ketahui:

- Jangka waktu normal - Sebagian besar transfer selesai dalam 5-7 hari, tetapi dapat memakan waktu hingga 10 hari.
- Memantau status transfer - Periksa kemajuan transfer Anda di konsol Route 53. Untuk informasi selengkapnya, lihat [Melihat status transfer domain](#).
- Menanggapi email dengan cepat - Kedua pendaftar dapat mengirim email konfirmasi yang memerlukan tanggapan Anda untuk melanjutkan.
- Hubungi registrar Anda saat ini - Jika transfer tertunda, hubungi registrar Anda saat ini untuk memastikan mereka tidak memblokir transfer.

Kapan harus menghubungi AWS Support

Hubungi AWS Support jika Anda sudah mencoba solusi di atas dan masih mengalami masalah, atau jika Anda mengalami:

- Kegagalan transfer setelah beberapa upaya dengan informasi yang benar
- Masalah penagihan atau pembayaran selama proses transfer
- Kesalahan teknis di konsol Route 53 yang mencegah Anda memulai transfer
- Transfer yang tetap dalam status “tertunda” selama lebih dari 10 hari

Saat Anda menghubungi dukungan, sertakan nama domain, ID permintaan transfer (jika tersedia), dan detail tentang kesalahan atau masalah tertentu yang Anda alami.

Mentransfer domain dari Amazon Route 53 ke registrar lain

Saat Anda mentransfer domain dari Amazon Route 53 ke registrar lain, Anda mendapatkan beberapa informasi dari Route 53 dan memberikannya ke registrar baru. Registrar baru akan melakukan sisanya.

Important

Jika saat ini Anda menggunakan Route 53 sebagai penyedia layanan DNS dan Anda juga ingin mentransfer layanan DNS ke penyedia lain, ketahuilah bahwa fitur Route 53 berikut tidak memiliki paralel langsung dengan fitur yang disediakan oleh penyedia layanan DNS lainnya. Anda harus bekerja dengan penyedia layanan DNS baru untuk menentukan cara mencapai fungsionalitas yang sebanding:

- Catatan alias. Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).
- Kebijakan perutean selain kebijakan perutean sederhana. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).
- Pemeriksaan kondisi yang terkait dengan catatan. Untuk informasi selengkapnya, lihat [Mengonfigurasi failover DNS](#).

Sebagian besar pendaftar domain memberlakukan persyaratan untuk mentransfer domain ke registrar lain. Tujuan utama dari persyaratan ini adalah untuk mencegah pemilik domain palsu agar tidak berulang kali mentransfer domain ke registrar yang berbeda. Persyaratan bervariasi, tetapi persyaratan berikut adalah khusus:

- Anda harus telah mendaftarkan domain dengan registrar saat ini atau mentransfer pendaftaran untuk domain ke registrar saat ini setidaknya 14 hari yang lalu.
- Domain tidak boleh memiliki salah satu dari kode status nama domain berikut:
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - clientTransferProhibited
 - serverTransferProhibited

Untuk daftar kode status nama domain saat ini dan penjelasan tentang arti setiap kode, kunjungi [situs web ICANN](#) dan cari kode status epp. (Penelusuran di situs web ICANN; penelusuran web terkadang mengembalikan versi dokumen yang lama.)

Note

Jika Anda ingin mentransfer domain Anda ke registrar domain lain tetapi AWS akun tempat domain terdaftar ditutup, ditangguhkan, atau dihentikan, Anda dapat menghubungi AWS Support untuk bantuan. Domain tidak dapat ditransfer dalam 14 hari pertama sejak pendaftaran. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

 Note

Jika registrar baru memerlukan kode REG-ID, Anda dapat menghubungi AWS Support untuk bantuan. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Untuk mentransfer domain dari Route 53 ke registrar lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pilih nama domain yang ingin Anda transfer ke registrar lain.
4. Pada halaman nama domain, periksa nilai kode status nama domain. Jika ini adalah salah satu nilai berikut, Anda tidak dapat mentransfer domain saat ini:
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - clientTransferProhibited
 - serverTransferProhibited

Untuk daftar kode status nama domain saat ini dan penjelasan tentang arti setiap kode, kunjungi [situs web ICANN](#) dan cari kode status epp. (Penelusuran di situs web ICANN; penelusuran web terkadang mengembalikan versi dokumen yang lama.)

Jika nilai kode status nama Domain adalah serverTransferProhibited, Anda dapat menghubungi AWS Support secara gratis untuk mempelajari apa yang harus Anda lakukan sehingga Anda dapat mentransfer domain. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

5. Jika nilai kunci Transfer Aktif, pilih Matikan kunci transfer dari dropdown Tindakan.
6. Semua domain kecuali domain.be, .co.za, .ru, .uk, .co.uk, .me.uk, dan .org.uk — Pada halaman nama domain, pilih Transfer ke registrar lain dari dropdown Transfer out.

Dalam kotak dialog Transfer ke registrar lain, pilih Salin untuk menyalin kode otorisasi untuk transfer domain. Anda akan memberikan nilai ini ke registrar Anda nanti dalam prosedur ini.

 Note

Untuk domain.eu, Anda juga dapat membuat kode autentikasi dengan menggunakan panel “my.eu” di registri: <https://my.eurid.eu/>.

.be, .co.za, .es, .ru, .uk, .co.uk, .me.uk, dan .org.uk domain - Lakukan hal berikut:

domain.be

[Dapatkan kode otorisasi dari registri untuk domain.be di situs web DNS Belgia.](#)

Domain .co.za

Anda tidak perlu mendapatkan kode otorisasi untuk mentransfer domain .co.za ke registrar lain.

Domain .ru

[Dapatkan kode otorisasi dari registri untuk domain .ru di https://www.nic.ru/en/auth/recovery/](https://www.nic.ru/en/auth/recovery/):

- Pilih opsi untuk memulihkan kredensial berdasarkan nama domain.
- Masukkan nama domain Anda, dan pilih Continue (Lanjutkan).
- Ikuti petunjuk di layar untuk mendapatkan akses ke halaman admin RU-CENTER.
- Di bagian Manage your account (Kelola akun Anda), pilih Domain transfer (Transfer domain).
- Konfirmasikan transfer dengan REGRU-RU.

Domain .uk, .co.uk, .me.uk, dan .org.uk

Ubah tanda IPS ke nilai registrar baru:

- Pergi ke [Temukan Panitera](#) di situs web Nominet, dan temukan tanda IPS untuk registrar baru. (Nominet adalah registri untuk domain.uk, .co.uk, .me.uk, dan .org.uk.)
- Pada halaman Domain Terdaftar > nama domain, pilih Transfer keluar, drop-down, lalu Perbarui Tag IPS, dan tentukan nilai yang Anda dapatkan di langkah 6a.
- Pilih Perbarui.

 Note

Anda juga dapat memperbarui tag IPS di konsol Nominet. Untuk petunjuk, lihat [Mengganti registrar](#).

7. Jika Anda saat ini tidak menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lewati ke langkah 10.

Jika saat ini Anda menggunakan Route 53 sebagai penyedia layanan DNS untuk domain, lakukan langkah-langkah berikut:

- a. Pilih Hosted Zones (Zona yang Di-hosting).
- b. Pilih nama zona yang di-hosting untuk domain Anda. Domain dan zona yang di-hosting memiliki nama yang sama.
- c. Jika Anda ingin terus menggunakan Route 53 sebagai penyedia layanan DNS untuk domain: Dapatkan nama dari empat server nama yang ditetapkan Route 53 ke zona yang di-hosting Anda. Untuk informasi selengkapnya, lihat [Mendapatkan server nama untuk zona yang di-hosting publik](#).

Jika Anda tidak ingin melanjutkan menggunakan Route 53 sebagai penyedia layanan DNS untuk domain: Catat pengaturan untuk semua catatan Anda kecuali catatan NS dan SOA. Untuk fitur khusus Route 53 seperti catatan alias, Anda harus bekerja dengan penyedia layanan DNS baru Anda untuk menentukan cara mencapai fungsionalitas yang sebanding.

8. Jika Anda mentransfer layanan DNS ke penyedia lain, gunakan metode yang disediakan oleh layanan DNS baru untuk melakukan tugas berikut:
 - Membuat zona yang di-hosting
 - Buat catatan yang mereproduksi fungsionalitas catatan Route 53 Anda
 - Dapatkan server nama yang ditetapkan oleh layanan DNS baru ke zona yang di-hosting Anda
9. Gunakan proses yang disediakan oleh registrar baru untuk meminta transfer domain.

Semua domain kecuali domain.co.za, .uk, .co.uk, .me.uk, dan .org.uk — Anda akan diminta untuk memasukkan kode otorisasi yang Anda dapatkan dari konsol Route 53 pada langkah 6 prosedur ini.

10. Jika Anda masih ingin menggunakan Route 53 sebagai penyedia layanan DNS Anda, gunakan proses yang disediakan oleh registrar baru untuk menentukan nama server nama Route 53

yang Anda dapatkan di langkah 7. Jika Anda ingin menggunakan penyedia layanan DNS lain, tentukan nama server nama yang diberikan penyedia baru saat Anda membuat zona host baru di langkah 8.

11. Merespons email konfirmasi:

Semua domain kecuali domain .jp

Route 53 mengirimkan email konfirmasi ke alamat email kontak pendaftar untuk domain:

- Jika Anda tidak membalas email, transfer terjadi secara otomatis pada tanggal yang ditentukan.
- Jika Anda ingin transfer terjadi lebih cepat atau Anda ingin membatalkan transfer, pilih tautan di email untuk membuka situs web Route 53, dan pilih opsi yang berlaku.
- Bergantung pada TLD, email konfirmasi mungkin berisi tautan ke <https://approvemove.com> tempat Anda dapat menyetujui atau menolak transfer. Ketika perlindungan privasi diaktifkan untuk kontak domain, email akan dikirimkan dari alamat identity-protect.org untuk terdaftar TLDs di Amazon Registrar. Untuk menentukan registrar TLD Anda, lihat [Menemukan registrar Anda](#).

Domain .jp

Route 53 mengirimkan email konfirmasi ke alamat email untuk kontak pendaftar untuk domain dari alamat noreply@domainnameverification.net atau noreply@emailverification.info dengan tautan untuk mengonfirmasi transfer:

- Jika Anda tidak merespons email tersebut, transfer dibatalkan pada tanggal yang ditentukan.
- Jika Anda ingin transfer terjadi lebih cepat atau Anda ingin membatalkan transfer, pilih tautan di email untuk membuka situs web Route 53, dan pilih opsi yang berlaku. Anda akan diminta untuk memberikan kode otorisasi domain yang Anda peroleh pada langkah 7.

Selain itu Anda mungkin menerima email dari WIXI.jp. Anda dapat mengabaikan email ini.

12. Jika registrar tempat Anda mentransfer domain melaporkan bahwa transfer gagal, hubungi registrar tersebut untuk informasi selengkapnya. Saat Anda mentransfer domain ke registrar lain, semua pembaruan status masuk ke registrar baru, jadi Route 53 tidak memiliki informasi tentang mengapa transfer gagal.

Jika registrar baru melaporkan bahwa transfer gagal karena kode otorisasi yang Anda dapatkan dari Route 53 tidak valid, buka kasus dengan AWS Support. (Anda tidak memerlukan kontrak

dukungan, dan tidak ada biaya.) Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

 Note

Kode otorisasi yang dihasilkan oleh Gandi berlaku selama sekitar 5 hari. Jika upaya transfer Anda terjadi setelah periode ini, mungkin gagal karena kode kedaluwarsa.

13. Jika Anda mentransfer layanan DNS ke penyedia layanan DNS lain, Anda dapat menghapus catatan di zona yang di-hosting dan menghapus zona yang di-hosting setelah DNS resolver berhenti merespons kueri DNS dengan nama server nama Route 53. Ini biasanya memakan waktu dua hari, jumlah waktu yang biasanya digunakan oleh DNS resolver untuk men-cache nama server nama untuk sebuah domain.

 Important

Jika Anda menghapus zona yang di-hosting saat DNS resolver masih merespons kueri DNS dengan nama server nama Route 53, domain Anda akan menjadi tidak tersedia di internet.

Setelah Anda menghapus zona yang di-hosting, Route 53 akan berhenti menagih Anda pada biaya bulanan untuk zona yang di-hosting. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- [Menghapus catatan](#)
- [Menghapus zona yang di-hosting publik](#)
- [Harga Route 53](#)

Mentransfer domain ke akun lain AWS

Jika Anda mendaftarkan domain menggunakan satu AWS akun dan Anda ingin mentransfer domain ke AWS akun lain, Anda dapat dengan mudah mentransfernya dengan menggunakan konsol baru, atau dengan menggunakan AWS CLI atau metode terprogram lainnya.

Topik

- [Langkah 1: Transfer domain ke AWS akun lain](#)

- [Langkah 2 \(Opsional\): Migrasikan zona yang dihosting ke akun lain AWS](#)

Langkah 1: Transfer domain ke AWS akun lain

Domain tidak dapat ditransfer dalam 14 hari pertama sejak pendaftaran.

Ketika Anda memulai transfer domain, Anda harus masuk baik dengan menggunakan akun root atau dengan menggunakan pengguna yang telah diberikan izin IAM dalam satu atau beberapa cara berikut:

- Pengguna diberi kebijakan AdministratorAccess terkelola.
- Pengguna diberi AmazonRoute53 kebijakan DomainsFullAccess terkelola.
- Pengguna diberi AmazonRoute53 kebijakan FullAccess terkelola.
- Pengguna diberi kebijakan PowerUserAccess terkelola.
- Pengguna memiliki izin untuk melakukan semua tindakan berikut: TransferDomains, DisableDomainTransferLock, dan RetrieveDomainAuthCode.

Jika Anda tidak masuk dengan menggunakan akun root atau dengan menggunakan pengguna yang memiliki izin yang diperlukan, kami tidak dapat melakukan transfer. Persyaratan ini mencegah pengguna yang tidak sah mentransfer domain ke domain lain. Akun AWS

Proses transfer memiliki dua langkah. Pertama pemilik akun asal memulai transfer: dalam [memulai transfer ke Akun AWS prosedur lain](#), dan kemudian pemilik akun tujuan menerima transfer dalam menerima [transfer dari](#) prosedur lain. Akun AWS

Untuk mentransfer domain ke AWS akun lain

1. Masuk AWS dengan menggunakan domain Akun AWS yang saat ini terdaftar.
2. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Domain terdaftar.
4. Pilih nama domain yang ingin Anda transfer ke yang lain Akun AWS.
5. Di atas bagian Detail, di dropdown Transfer out, pilih Transfer ke yang lain. Akun AWS
6. Pada Akun AWS dialog Transfer ke yang lain, masukkan ID akun tujuan. Anda bisa mendapatkan ID ini dari Akun AWS pemilik tujuan.
7. Pilih Konfirmasi.

8. Pada dialog Hasilkan kata sandi, salin kata sandi, dan teruskan ke Akun AWS pemilik penerima.

Pada halaman Permintaan, Status untuk domain akan ditampilkan Dalam proses, dan Jenis akan menampilkan Transfer internal keluar.

Untuk menerima transfer domain dari AWS akun yang berbeda

1. Masuk AWS dengan menggunakan Akun AWS yang menerima domain.
2. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Permintaan.
4. Pada halaman Permintaan, pilih tombol radio di sebelah nama domain yang Anda transfer dari yang lain Akun AWS. Jika domain siap ditransfer, Status adalah Tindakan yang diperlukan dan Tipe adalah Transfer internal domain di.

Anda memiliki tiga hari untuk menerima permintaan. Jika transfer tidak diterima dalam tiga hari, permintaan transfer dibatalkan.

5. Di dropdown Action, pilih Accept.

Anda juga dapat memilih Tolak untuk membatalkan proses transfer.

6. Jika Anda menerima, pada halaman Transfer domain ke akun Anda, di bagian Kata Sandi, masukkan kata sandi yang Anda terima dari pemilik akun asal.

Terima syarat dan ketentuan, dan pilih Berikutnya.

7. Arahkan ke halaman Permintaan untuk memantau status transfer dan langkah-langkah lain yang harus diselesaikan.
8. Setelah transfer selesai, Anda dapat memperbarui informasi kontak. Untuk informasi selengkapnya, lihat [Memperbarui informasi kontak dan kepemilikan domain](#).

Transfer domain secara terprogram

Anda juga dapat mentransfer domain secara terprogram dengan menggunakan AWS CLI, salah satu AWS SDKs, atau Route 53 API. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Untuk ikhtisar proses transfer dan dokumentasi tentang tindakan API yang Anda gunakan untuk mentransfer domain menggunakan API pendaftaran domain Route 53, lihat [TransferDomainToAnotherAwsAccount](#) di Referensi API Amazon Route 53.

- Untuk dokumentasi tentang opsi lain untuk mentransfer domain secara terprogram, lihat "SDKs & Toolkit" di bagian [Panduan dan Referensi API](#) di halaman "dokumentasi".AWS
- Akun penerima memiliki waktu tiga hari untuk menerima transfer dari akun asal, dengan menggunakan API [transfer-domain-to-another-aws-account](#). Jika transfer tidak diterima dalam tiga hari, permintaan transfer dibatalkan.

 Important

Saat Anda mentransfer domain ke AWS akun lain, zona yang dihosting untuk domain tidak ditransfer. Jika Anda juga ingin mentransfer zona yang di-hosting, tunggu hingga domain telah ditransfer, lalu lihat [Langkah 2 \(Opsional\): Migrasikan zona yang dihosting ke akun lain AWS](#).

Langkah 2 (Opsional): Migrasikan zona yang dihosting ke akun lain AWS

Jika Anda menggunakan Route 53 sebagai layanan DNS untuk domain, Route 53 tidak mentransfer zona yang dihosting saat Anda mentransfer domain ke AWS akun lain. Jika pendaftaran domain dikaitkan dengan satu akun dan zona yang di-hosting terkait dikaitkan dengan akun lain, baik pendaftaran domain maupun fungsionalitas DNS tidak terpengaruh. Satu-satunya efek adalah Anda harus masuk ke konsol Route 53 menggunakan satu akun untuk melihat domain, dan masuk menggunakan akun lain untuk melihat zona yang di-hosting.

Jika Anda memiliki akun tempat Anda mentransfer domain dan akun tempat Anda mentransfer domain, Anda dapat secara opsional memigrasikan zona yang di-hosting untuk domain ke akun lain, tetapi itu tidak diperlukan. Route 53 akan terus menggunakan catatan di zona host yang ada untuk merutekan lalu lintas untuk domain.

 Important

Jika Anda tidak memiliki akun tempat Anda mentransfer domain dan akun tempat Anda mentransfer domain, Anda harus memigrasikan zona host yang ada ke AWS akun tempat Anda mentransfer domain, atau membuat zona host baru di AWS akun yang Anda miliki. Jika Anda tidak memiliki akun yang membuat zona yang di-hosting yang merutekan lalu lintas untuk domain, Anda tidak dapat mengontrol bagaimana lalu lintas dirutekan.

Untuk memigrasi zona yang di-hosting yang ada ke akun baru, lihat [Migrasi zona yang dihosting ke akun lain AWS](#).

Untuk membuat zona yang di-hosting baru, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#). Topik ini biasanya digunakan saat Anda mentransfer domain dari registrar lain ke Route 53, tetapi prosesnya sama saat Anda mentransfer domain dari satu akun ke akun lainnya. AWS

Important

Server nama label putih: Jika domain Anda menggunakan server nama label putih (nama host server nama khusus seperti ns1.example.com), diperlukan langkah-langkah tambahan:

- Saat mentransfer pendaftaran domain: Perbarui catatan lem dengan registrar baru Anda setelah transfer selesai
- Saat memigrasi zona yang dihosting: Perbarui catatan lem dengan registrar domain Anda setelah migrasi zona, karena alamat IP berubah meskipun nama host tetap sama

Untuk petunjuk mendetail, lihat [the section called “Langkah 7: Membuat glue record dan mengubah server nama registrar”](#).

Melihat status transfer domain

Setelah Anda memulai transfer domain dari registrar domain lain ke Amazon Route 53, Anda dapat melacak status pada halaman Permintaan (konsol baru) atau halaman Permintaan tertunda (konsol lama) dari konsol Route 53. Kolom Status menyertakan deskripsi singkat tentang langkah saat ini. Daftar berikut menyertakan teks di konsol dan deskripsi yang lebih mendetail dari setiap langkah.

Note

Saat Anda mengirimkan permintaan transfer, status awalnya adalah Permintaan transfer domain terkirim, yang menunjukkan bahwa kami telah menerima permintaan Anda.

Menentukan apakah domain memenuhi persyaratan transfer (langkah 1 dari 14)

Kami mengonfirmasi bahwa status domain Anda memenuhi syarat untuk ditransfer. Anda harus membuka kunci domain, dan domain tidak boleh memiliki salah satu kode status berikut saat Anda mengirimkan permintaan transfer:

- `clientTransferProhibited`
- `pendingDelete`
- `pendingTransfer`
- `redemptionPeriod`

TLDs Hanya geografis — memverifikasi informasi WHOIS (langkah 2 dari 14)

Jika Anda mentransfer domain yang memiliki [TLD geografis](#), kami mengirimkan kueri WHOIS untuk domain Anda guna menentukan apakah Anda telah menonaktifkan perlindungan privasi untuk domain tersebut. Jika perlindungan privasi masih diaktifkan dengan registrar Anda saat ini, kami tidak akan dapat mengakses informasi yang kami perlukan untuk mentransfer domain.

Note

Otorisasi tidak diperlukan untuk domain yang memiliki [TLD umum](#), seperti `.com`, `.net`, atau `.org`.

TLDs Hanya geografis - Mengirim email ke kontak pendaftar untuk mendapatkan otorisasi transfer (langkah 3 dari 14)

Jika Anda mentransfer domain yang memiliki [TLD geografis](#), kami telah mengirimkan email ke kontak pendaftar untuk domain tersebut. Tujuan email tersebut adalah untuk mengonfirmasi bahwa transfer diminta oleh kontak resmi domain tersebut.

Note

Otorisasi tidak diperlukan untuk domain yang memiliki [TLD umum](#), seperti `.com`, `.net`, atau `.org`.

Memverifikasi transfer dengan registrar saat ini (langkah 4 dari 14)

Kami telah mengirimkan permintaan ke registrar saat ini untuk domain agar dapat memulai transfer.

TLDs Hanya geografis - Menunggu otorisasi dari kontak pendaftar (langkah 5 dari 14)

Kami mengirim email ke kontak pendaftar untuk domain tersebut (lihat langkah 3 dari 14), dan kami menunggu kontak pendaftar mengklik tautan di email untuk mengotorisasi transfer. Jika Anda mentransfer domain yang memiliki [TLD geografis](#) dan Anda tidak menerima email karena alasan tertentu, lihat [Mengirim ulang email otorisasi dan konfirmasi](#).

Contacted current registrar to request transfer (step 6 of 14)

Kami sedang bekerja dengan pencatat domain saat ini untuk menyelesaikan transfer.

Menunggu pendaftar saat ini menyelesaikan transfer (langkah 7 dari 14)

Registrar Anda saat ini mengonfirmasi bahwa domain Anda memenuhi persyaratan untuk ditransfer. Langkah ini mungkin memerlukan waktu hingga sepuluh hari, bergantung pada TLD untuk domain Anda:

- [Domain tingkat atas generik](#) – memakan waktu hingga tujuh hari
- [Domain tingkat atas geografis](#) (juga dikenal sebagai domain tingkat atas kode negara) – membutuhkan waktu hingga sepuluh hari

Note

Jika Anda telah menyetujui email konfirmasi yang dikirim dari Route 53 saat mentransfer domain.JP, tetapi telah berhenti selama beberapa hari di LANGKAH 7, hubungi [AWS Support Center](#) untuk bantuan.

Untuk sebagian besar registrar, prosesnya sepenuhnya otomatis dan tidak dapat dipercepat. Beberapa registrar mengirimkan email yang meminta Anda menyetujui transfer; Jika registrar Anda mengirimkan email konfirmasi ini, proses transfer mungkin jauh lebih cepat dari tujuh hingga sepuluh hari.

Untuk informasi tentang alasan registrar menolak transfer, lihat [Persyaratan transfer untuk domain tingkat atas](#).

Mengonfirmasi dengan kontak pendaftar bahwa kontak tersebut yang memulai transfer (langkah 8 dari 14)

Beberapa pendaftar TLD mengirim pendaftar menghubungi email lain untuk mengonfirmasi bahwa transfer domain diminta oleh pengguna yang berwenang.

Menyinkronkan server nama dengan registri (langkah 9 dari 14)

Langkah ini terjadi hanya jika server nama yang Anda berikan sebagai bagian dari permintaan transfer berbeda dari server nama yang terdaftar dengan pencatat saat ini. Kami akan mencoba memperbarui server nama Anda ke server nama baru yang Anda berikan.

Menyinkronkan pengaturan dengan registri (langkah 10 dari 14)

Kami memverifikasi bahwa transfer telah berhasil diselesaikan, dan kami menyinkronkan data terkait domain Anda dengan rekan registrar kami.

Mengirim informasi kontak diperbarui ke registri (langkah 11 dari 14)

Jika Anda mengubah kepemilikan domain saat meminta transfer, kami mencoba melakukan perubahan ini. Namun, sebagian besar registri tidak mengizinkan transfer kepemilikan sebagai bagian dari proses transfer domain.

Menyelesaikan transfer ke Route 53 (langkah 12 dari 14)

Kami mengonfirmasikan bahwa proses transfer berhasil.

Menyelesaikan transfer (langkah 13 dari 14)

Kami menyiapkan domain Anda di Route 53.

Transfer Selesai (langkah 14 dari 14)

Transfer Anda telah berhasil diselesaikan.

Cara mentransfer domain ke Amazon Route 53 memengaruhi tanggal kedaluwarsa pendaftaran domain Anda

Saat Anda mentransfer domain antarregistrar, beberapa pendaftar TLD memungkinkan Anda menyimpan tanggal kedaluwarsa yang sama untuk domain Anda, beberapa pendaftar menambahkan satu tahun ke tanggal kedaluwarsa, dan beberapa pendaftar mengubah tanggal kedaluwarsa menjadi satu tahun setelah tanggal transfer.

Note

Untuk sebagian besar TLDs, Anda dapat memperpanjang periode pendaftaran untuk domain hingga sepuluh tahun setelah Anda mentransfernya ke Amazon Route 53. Untuk informasi selengkapnya, lihat [Memperpanjang masa pendaftaran untuk domain](#).

Generik TLDs

Saat Anda mentransfer domain yang memiliki TLD umum (misalnya, .com) ke Route 53, tanggal kedaluwarsa yang baru untuk domain tersebut adalah tanggal kedaluwarsa dengan pencatat Anda sebelumnya ditambah satu tahun.

Geografis TLDs

Saat Anda mentransfer domain yang memiliki TLD geografis (misalnya, .co.uk) ke Route 53, tanggal kedaluwarsa yang baru untuk domain bergantung pada TLD. Temukan TLD Anda di tabel berikut untuk menentukan bagaimana transfer domain memengaruhi tanggal kedaluwarsa.

Benua	Geografis TLDs dan efek transfer domain pada tanggal kedaluwarsa
Afrika	.co.za – Tanggal kedaluwarsa tetap sama.
Amerika	.cl, .com.ar, .com.br – Tanggal kedaluwarsa tetap sama. .ca, .co, .mx, .us – Satu tahun ditambahkan ke tanggal kedaluwarsa lama.
Asia/Oseania	.com.au, .com.sg, .jp, .net.au, .sg — Tanggal kedaluwarsa tetap sama. .co.nz, .in, .net.nz, .org.nz - Satu tahun ditambahkan ke tanggal kedaluwarsa lama.
Europa	.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se – Tanggal kedaluwarsa tetap sama. .berlin, .eu, .io, .me, .ruhr, .wien – Satu tahun ditambahkan ke tanggal kedaluwarsa lama. .be, .de, .fr, .it, .nl – Tanggal kedaluwarsa yang baru adalah satu tahun setelah tanggal transfer.

Mengirim ulang email otorisasi dan konfirmasi

Untuk beberapa operasi terkait pendaftaran domain, ICANN mewajibkan kami mendapatkan otorisasi dari kontak pendaftar untuk domain tersebut atau konfirmasi bahwa alamat email untuk kontak pendaftar sudah valid. Untuk mendapatkan otorisasi atau konfirmasi, kami mengirim email yang berisi tautan. Anda memiliki waktu antara 3 hingga 15 hari untuk mengeklik tautan, tergantung operasi dan domain tingkat atas. Setelah waktu tersebut, tautan berhenti bekerja.

Jika Anda tidak mengeklik tautan pada email dalam waktu yang ditentukan, ICANN umumnya mengharuskan kami menangguhkan domain atau membatalkan operasi, tergantung pada hal yang Anda coba lakukan:

Mendaftarkan domain

Domain ditangguhkan sehingga tidak dapat diakses di internet. Untuk mengirim ulang email konfirmasi, lihat [Cara mengirim ulang email konfirmasi untuk pendaftaran domain](#).

TLDs Hanya geografis - Transfer domain ke Amazon Route 53

Jika Anda mentransfer domain yang memiliki [TLD geografis](#), kami membatalkan transfer. Untuk mengirim ulang email otorisasi, lihat [Cara mengirim ulang email otorisasi untuk transfer domain](#).

Note

Otorisasi tidak diperlukan untuk domain yang memiliki [TLD umum](#), seperti .com, .net, atau .org.

Mengubah nama atau alamat email kontak pendaftar untuk domain (pemilik)

Kami membatalkan perubahan. Untuk mengirim ulang email otorisasi, lihat [Cara mengirim ulang email otorisasi untuk memperbarui kontak pendaftar atau menghapus domain](#).

Menghapus domain

Kami membatalkan permintaan penghapusan. Untuk mengirim ulang email otorisasi, lihat [Cara mengirim ulang email otorisasi untuk memperbarui kontak pendaftar atau menghapus domain](#).

TLDs Hanya geografis — Transfer domain dari Route 53 ke registrar lain

Jika Anda mentransfer domain yang memiliki [TLD geografis](#), registrar baru membatalkan transfer.

 Note

Otorisasi tidak diperlukan untuk domain yang memiliki [TLD umum](#), seperti .com, .net, atau .org.

Topik

- [Memperbarui alamat email](#)
- [Mengirim ulang email](#)

Memperbarui alamat email

Kami selalu mengirim email konfirmasi dan otorisasi ke alamat email untuk kontak pendaftar domain. Untuk beberapa orang TLDs, kami diminta untuk mengirim email ke alamat email lama dan baru untuk kontak pendaftar dalam kasus berikut:

- Anda mengubah alamat email untuk domain yang sudah terdaftar dengan Amazon Route 53
- Anda mengubah alamat email untuk domain yang ditransfer ke Route 53

Mengirim ulang email

Gunakan prosedur yang berlaku untuk mengirim ulang email konfirmasi atau otorisasi.

- [Cara mengirim ulang email konfirmasi untuk pendaftaran domain](#)
- [Cara mengirim ulang email otorisasi untuk transfer domain](#)
- [Cara mengirim ulang email otorisasi untuk memperbarui kontak pendaftar atau menghapus domain](#)

Cara mengirim ulang email konfirmasi untuk pendaftaran domain

1. Periksa alamat email untuk kontak pendaftar dan, jika perlu, perbarui alamat email. Untuk informasi selengkapnya, lihat [Memperbarui informasi kontak dan kepemilikan domain](#).
2. Periksa folder spam di aplikasi email Anda untuk mendapatkan email dari salah satu alamat email berikut.

Jika waktu sudah terlewat, tautan tidak akan berfungsi lagi, tetapi Anda akan tahu tempat mencari email konfirmasi ketika kami mengirimkan email lainnya kepada Anda.

TLDs	Alamat email tempat asal email persetujuan atau konfirmasi
.fr	nic@nic.fr
Semua yang lain	Salah satu alamat email berikut: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

 Note

Email tersebut mungkin berisi tautan ke www.verify-whois.com. Tautan ini aman digunakan.

3. Gunakan konsol Amazon Route 53 untuk mengirim ulang email konfirmasi:
 - a. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 - b. Di panel navigasi, pilih Domain terdaftar.
 - c. Pilih nama domain yang ingin Anda kirimkan ulang email.
 - d. Di kotak peringatan dengan judul "Domain Anda mungkin ditangguhkan," pilih Kirim email lagi.

 Note

Jika tidak ada kotak peringatan, Anda telah mengonfirmasi bahwa alamat email untuk kontak pendaftar sudah valid.

4. Jika Anda mengalami masalah saat mengirim ulang email konfirmasi, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Cara mengirim ulang email otorisasi untuk transfer domain

Metode ini tidak berfungsi untuk permintaan transfer keluar domain .jp.

1. Gunakan metode yang disediakan oleh registrar domain saat ini untuk mengonfirmasi bahwa perlindungan privasi untuk domain dinonaktifkan. Jika tidak, nonaktifkan.

Kami mengirim email otorisasi ke alamat email yang disimpan registrar saat ini dalam basis data WHOIS. Ketika perlindungan privasi diaktifkan, alamat email tersebut biasanya dikaburkan. Registrar saat ini mungkin tidak meneruskan email yang dikirim Amazon Route 53 ke alamat email di basis data WHOIS ke alamat email Anda yang sebenarnya.

Note

Jika registrar domain saat ini tidak mengizinkan Anda menonaktifkan perlindungan privasi, kami tetap dapat mentransfer domain jika Anda menentukan kode otorisasi yang valid di [Langkah 5: Minta transfer](#).

2. Periksa alamat email untuk kontak pendaftar dan, jika perlu, perbarui alamat email. Gunakan metode yang disediakan oleh registrar domain saat ini.
3. Periksa folder spam di aplikasi email Anda untuk mendapatkan email dari salah satu alamat email berikut.

Jika waktu sudah terlewat, tautan tidak akan berfungsi lagi, tetapi Anda akan tahu tempat mencari email otorisasi ketika kami mengirimkan email lainnya kepada Anda.

TLDS	Alamat email tempat asal email persetujuan atau konfirmasi
.com.au dan .net.au	no-reply@ispapi.net Email berisi tautan ke https://approve.domainadmin.com .
.fr	nic@nic.fr

TLDs	Alamat email tempat asal email persetujuan atau konfirmasi
Semua yang lain	Salah satu alamat email berikut: • <code>noreply@registrar.amazon</code> • <code>noreply@domainnameverification.net</code> • <code>noreply@emailverification.info</code>

 Note

Email tersebut mungkin berisi tautan ke www.verify-whois.com. Tautan ini aman digunakan.

4. Jika proses transfer tidak lagi berjalan (jika kami membatalkannya karena waktunya sudah terlewat), minta transfer lagi, dan kami akan mengirimkan email otorisasi lain kepada Anda.

 Note

Selama 15 hari pertama setelah meminta transfer, Anda dapat menentukan status transfer dengan memeriksa tabel Notifikasi dalam halaman Dasbor di konsol Route 53. Setelah 15 hari, gunakan AWS CLI untuk mendapatkan status. Untuk informasi lebih lanjut, lihat [route53domains](#) dalam Referensi Perintah AWS CLI .

Jika transfer masih berlangsung, lakukan langkah berikut untuk mengirim ulang email otorisasi.

- a. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
- b. Di tabel Notifikasi, temukan domain yang ingin Anda transfer.
- c. Di kolom Status domain tersebut, pilih Kirim ulang email.

5. Jika Anda mengalami masalah saat mengirim ulang email otorisasi untuk transfer domain, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Cara mengirim ulang email otorisasi untuk memperbarui kontak pendaftar atau menghapus domain

1. Periksa alamat email untuk kontak pendaftar dan, jika perlu, perbarui alamat email. Untuk informasi selengkapnya, lihat [Memperbarui informasi kontak dan kepemilikan domain](#).
2. Periksa folder spam di aplikasi email Anda untuk mendapatkan email dari salah satu alamat email berikut.

Jika waktu sudah terlewat, tautan tidak akan berfungsi lagi, tetapi Anda akan tahu tempat mencari email otorisasi ketika kami mengirimkan email lainnya kepada Anda.

TLDs	Alamat email tempat asal email otorisasi
.fr	nic@nic.fr
Semua yang lain	Salah satu alamat email berikut: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

 Note

Email tersebut mungkin berisi tautan ke www.verify-whois.com. Tautan ini aman digunakan.

3. Membatalkan perubahan atau penghapusan. Anda memiliki dua opsi:

- Anda dapat menunggu hingga periode tunggu 3 hingga 15 hari berakhir, setelah itu kami secara otomatis membatalkan operasi yang diminta.
- Atau, Anda dapat menghubungi AWS Support dan meminta mereka untuk membatalkan operasi.

Important

Jenis transfer dan metode pembatalan: Metode pembatalan tergantung pada jenis transfer:

- Registrar eksternal ke Route 53: Ikuti prosedur dalam topik ini (tunggu pembatalan otomatis atau hubungi Support) AWS
- Antar AWS akun: Gunakan `CancelDomainTransferToAnotherAwsAccount` API atau hubungi AWS Support

Jangan menghubungi pencatat eksternal Anda saat ini untuk membatalkan transfer ke Route 53, karena mereka tidak dapat membatalkan transfer yang sudah berlangsung. AWS

4. Setelah perubahan atau penghapusan dibatalkan, Anda dapat mengubah informasi kontak atau menghapus domain lagi, dan kami akan mengirimkan email otorisasi lain kepada Anda.
5. Jika Anda mengalami masalah saat mengirim ulang email otorisasi, Anda dapat menghubungi AWS Support secara gratis. Lihat informasi yang lebih lengkap di [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Mengonfigurasi DNSSEC untuk domain

Penyerang terkadang membajak lalu lintas ke titik akhir internet seperti server web dengan mencegat kueri DNS dan mengembalikan alamat IP penyerang ke penyelesai DNS menggantikan alamat IP yang sebenarnya untuk titik akhir tersebut. Pengguna kemudian dirutekan ke alamat IP yang disediakan oleh penyerang sebagai respons palsu, misalnya, ke situs web palsu.

Anda dapat melindungi domain Anda dari jenis serangan ini, yang dikenal sebagai spoofing DNS atau man-in-the-middle serangan, dengan mengonfigurasi Domain Name System Security Extensions (DNSSEC), sebuah protokol untuk mengamankan lalu lintas DNS.

 Important

Amazon Route 53 mendukung penandatanganan DNSSEC dan DNSSEC untuk pendaftaran domain. Jika Anda ingin mengonfigurasi penandatanganan DNSSEC untuk domain yang terdaftar dengan Route 53, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

Topik

- [Gambaran umum tentang cara DNSSEC melindungi domain Anda](#)
- [Prasyarat dan nilai maksimal untuk mengonfigurasi DNSSEC domain](#)
- [Menambahkan kunci publik untuk domain](#)
- [Menghapus kunci publik untuk domain](#)

Gambaran umum tentang cara DNSSEC melindungi domain Anda

Saat Anda mengonfigurasi DNSSEC untuk domain, penyelesai DNS menetapkan rantai kepercayaan untuk respons dari penyelesai perantara. Rantai kepercayaan dimulai dengan registri TLD untuk domain (zona induk domain) dan diakhiri dengan server nama otoritatif di penyedia layanan DNS. Tidak semua penyelesai DNS mendukung DNSSEC. Hanya resolver yang mendukung DNSSEC yang melakukan validasi tanda tangan atau keaslian apa pun.

Berikut adalah cara mengonfigurasi DNSSEC untuk domain yang terdaftar di Amazon Route 53 guna melindungi host internet Anda dari DNS palsu, yang disederhanakan agar lebih jelas:

1. Gunakan metode yang disediakan oleh penyedia layanan DNS Anda untuk menandatangani catatan di zona yang di-hosting dengan kunci privat dalam pasangan kunci asimetris.

 Important

Route 53 mendukung penandatanganan DNSSEC dan DNSSEC untuk pendaftaran domain. Untuk mempelajari selengkapnya, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

2. Berikan kunci publik dari pasangan kunci ke registrar domain Anda, dan tentukan algoritme yang digunakan untuk menghasilkan pasangan kunci. Registrar domain meneruskan kunci publik dan algoritme ke registri untuk domain tingkat atas (TLD).

Untuk informasi tentang cara melakukan langkah ini untuk domain yang Anda daftarkan dengan Route 53, lihat [Menambahkan kunci publik untuk domain](#).

Setelah dikonfigurasi, berikut adalah cara DNSSEC melindungi domain Anda dari DNS palsu:

1. Kirim kueri DNS, misalnya, dengan menelusuri situs web atau mengirim pesan email.
2. Permintaan dirutekan ke penyelesai DNS. Penyelesai bertanggung jawab untuk mengembalikan nilai yang sesuai ke klien berdasarkan permintaan, misalnya, alamat IP untuk host yang menjalankan server web atau server email.
3. Jika alamat IP di-cache pada DNS resolver karena orang lain telah mengirimkan query DNS yang sama, dan resolver sudah mendapatkan nilai, resolver mengembalikan alamat IP ke klien yang mengirimkan permintaan. Klien kemudian menggunakan alamat IP untuk mengakses host.

Jika alamat IP tidak di-cache di penyelesai DNS, penyelesai mengirimkan permintaan ke zona induk domain Anda, di registri TLD, yang mengembalikan dua nilai:

- Catatan Delegation Signer (DS), yang merupakan kunci publik yang sesuai dengan kunci privat yang digunakan untuk menandatangani catatan.
 - Alamat IP dari server nama otoritatif untuk domain Anda.
4. Penyelesai DNS mengirimkan permintaan asli untuk penyelesai DNS lain. Jika tidak memiliki alamat IP, penyelesai itu mengulangi proses hingga penyelesai mengirimkan permintaan ke server nama di penyedia layanan DNS Anda. Server nama mengembalikan dua nilai:
 - Catatan untuk domain, seperti example.com. Biasanya ini berisi alamat IP host.
 - Tanda tangan untuk catatan, yang Anda buat saat mengonfigurasi DNSSEC.
 5. DNS resolver menggunakan kunci publik yang Anda berikan ke registrar domain dan registrar yang diteruskan ke registri TLD untuk melakukan dua hal:
 - Membuat rantai kepercayaan.
 - Verifikasi bahwa respons yang ditandatangani dari penyedia layanan DNS adalah sah dan belum diganti dengan respons buruk dari penyerang.
 6. Jika respons otentik, penyelesai mengembalikan nilai ke klien yang mengirimkan permintaan.

Jika respons tidak dapat diverifikasi, penyelesai mengembalikan kesalahan ke pengguna.

Jika registri TLD untuk domain tidak memiliki kunci publik untuk domain, penyelesai merespons kueri DNS menggunakan respons yang didapat dari penyedia layanan DNS.

Prasyarat dan nilai maksimal untuk mengonfigurasi DNSSEC domain

Untuk mengonfigurasi DNSSEC domain, domain dan penyedia layanan DNS harus memenuhi prasyarat berikut:

- Registri untuk TLD harus mendukung DNSSEC. Untuk menentukan apakah registri untuk TLD mendukung DNSSEC, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).
- Penyedia layanan DNS untuk domain harus mendukung DNSSEC.

Important

Route 53 mendukung penandatanganan DNSSEC dan DNSSEC untuk pendaftaran domain. Untuk mempelajari selengkapnya, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

- Anda harus mengonfigurasi DNSSEC dengan penyedia layanan DNS untuk domain sebelum menambahkan kunci publik domain ke Route 53.
- Jumlah kunci publik yang dapat Anda tambahkan ke domain tergantung pada TLD untuk domain:
 - Domain .com dan .net – hingga tiga belas kunci
 - Semua domain lainnya – hingga empat kunci

Menambahkan kunci publik untuk domain

Ketika Anda merotasi kunci atau mengaktifkan DNSSEC untuk domain, lakukan prosedur berikut setelah mengonfigurasi DNSSEC dengan penyedia layanan DNS untuk domain.

Cara menambahkan kunci publik untuk domain

1. Jika Anda belum mengonfigurasi DNSSEC dengan penyedia layanan DNS, gunakan metode yang disediakan oleh penyedia layanan untuk mengonfigurasi DNSSEC.
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Domain terdaftar.
4. Pilih nama domain yang ingin Anda tambahkan kunci.
5. Di tab Tombol DNSSEC, pilih Tambah kunci.
6. Tentukan nilai-nilai berikut ini:

Tipe Kunci

Pilih apakah Anda ingin mengunggah kunci penandatanganan kunci (KSK) atau kunci penandatanganan zona (ZSK).

Algoritme

Pilih algoritme yang Anda gunakan untuk menandatangani catatan zona yang di-hosting.

Kunci publik

Tentukan kunci publik dari pasangan kunci asimetris yang Anda gunakan untuk mengonfigurasi DNSSEC dengan penyedia layanan DNS.

Perhatikan hal berikut:

- Tentukan kunci publik, bukan digest.
- Anda harus menentukan kunci dalam format base64.

7. Pilih Tambahkan.

Note

Anda hanya dapat menambahkan satu kunci publik dalam satu waktu. Jika perlu menambahkan kunci lainnya, tunggu hingga Anda menerima email konfirmasi dari Route 53.

8. Saat Route 53 menerima respons dari registri, kami akan mengirim email ke kontak pendaftar untuk domain tersebut. Email ini menegaskan bahwa kunci publik telah ditambahkan ke domain di registri atau menjelaskan mengapa kunci tidak dapat ditambahkan.

Menghapus kunci publik untuk domain

Ketika Anda merotasi tombol atau menonaktifkan DNSSEC untuk domain, hapus kunci publik menggunakan prosedur berikut sebelum menonaktifkan DNSSEC dengan penyedia layanan DNS. Perhatikan hal berikut:

- Jika Anda merotasi kunci publik, sebaiknya tunggu hingga tiga hari setelah menambahkan kunci publik baru untuk menghapus kunci publik lama.

- Jika Anda menonaktifkan DNSSEC, hapus kunci publik untuk domain terlebih dahulu. Kami sarankan Anda menunggu hingga tiga hari sebelum menonaktifkan DNSSEC dengan layanan DNS untuk domain.

 Important

Jika DNSSEC diaktifkan untuk domain dan Anda menonaktifkan DNSSEC dengan layanan DNS, penyelesaian DNS yang mendukung DNSSEC akan mengembalikan kesalahan SERVFAIL untuk klien, dan klien tidak akan dapat mengakses titik akhir yang terkait dengan domain.

Cara menghapus kunci publik untuk domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pilih nama domain yang kuncinya ingin Anda hapus.
4. Di tab Tombol DNSSEC, pilih tombol radio di sebelah tombol yang ingin Anda hapus, lalu pilih Hapus kunci.
5. Dalam kotak dialog Delete DNSSEC key, masukkan hapus di kotak teks untuk mengonfirmasi bahwa Anda ingin menghapus kunci, lalu pilih Hapus.

 Note

Anda hanya dapat menghapus satu kunci publik dalam satu waktu. Jika Anda perlu menghapus lebih banyak kunci, tunggu hingga Anda menerima email konfirmasi dari Amazon Route 53.

6. Saat Route 53 menerima respons dari registri, kami akan mengirim email ke kontak pendaftar untuk domain tersebut. Email ini menegaskan bahwa kunci publik telah dihapus dari domain di registri atau menjelaskan mengapa kunci tidak dapat dihapus.

Menemukan registrar Anda dan informasi lain tentang domain Anda

Untuk melihat informasi domain dengan menggunakan [GetDomainDetail](#) API, Anda dapat menggunakan salah satu SDKs atau AWS CLI. Untuk informasi selengkapnya, lihat [get-domain-detail](#).

Untuk melihat informasi tentang domain dengan **get-domain-detail** CLI

- Gunakan CLI berikut:

```
aws route53domains get-domain-detail \
  --region us-east-1 \
  --domain-name example.com
```

Note

Perintah ini hanya berjalan di us-east-1 Wilayah AWS.

Semua informasi tentang domain Anda akan tercantum dalam output, termasuk registrar, tanggal pendaftaran, pengaturan privasi, dll.

Melihat informasi tentang domain yang terdaftar di Route 53

Note

Efektif 28 Januari 2025, beberapa pendaftar domain dapat beralih dari WHOIS ke Registration Data Access Protocol (RDAP) untuk kueri data pendaftaran domain. Jika Anda mengakses informasi pendaftaran domain langsung dari pendaftar melalui WHOIS, Anda mungkin perlu memperbarui aplikasi Anda untuk menggunakan titik akhir RDAP jika registri yang relevan menghentikan dukungan WHOIS.

Fungsionalitas layanan domain Route 53 tetap tidak berubah. Pemberitahuan ini hanya berlaku untuk kueri WHOIS registri langsung yang dilakukan di luar layanan Route 53.

Anda dapat melihat informasi tentang domain yang terdaftar menggunakan Route 53. Informasi ini mencakup rincian seperti ketika domain awalnya terdaftar dan informasi kontak untuk pemilik domain dan untuk kontak teknis, administratif, dan penagihan.

WHOIS

WHOIS adalah direktori gratis yang tersedia untuk umum yang berisi informasi tentang domain yang disponsori oleh pendaftar dan pendaftar domain. Ini disediakan sebagai layanan yang menerima kueri pada port 43, dan sebagai situs web, masing-masing dapat diakses melalui keduanya IPv4 dan IPv6. WHOIS adalah pencarian hierarkis terdistribusi. Untuk informasi lebih lanjut, lihat [Tentang WHOIS](#).

Permintaan WHOIS ke berbagai tingkat hierarki dapat memberikan informasi yang berbeda:

- Permintaan ke root WHOIS (whois.iana.org) memberikan informasi tentang registri.
- Permintaan untuk registri WHOIS memberikan informasi tentang registrar, dan beberapa informasi publik tentang domain.
- Permintaan untuk mendaftarkan WHOIS menyediakan semua informasi publik tentang domain.

Karena ada beberapa tingkatan WHOIS, termasuk pencarian WHOIS yang dioperasikan oleh registri TLD dan registrar domain, mematikan perlindungan privasi Anda di konsol Route 53 hanya dapat mematkannya pada WHOIS yang disediakan registrar. Beberapa pendaftar sengaja menjaga perlindungan privasi atau layanan redaksi untuk layanan pencarian WHOIS mereka terlepas dari apakah Anda telah mematkannya dengan Route 53. Untuk mendapatkan informasi lengkap tentang domain Anda, kami sarankan Anda menggunakan WHOIS yang disediakan registrar.

Perhatikan hal-hal berikut:

Mengirim email ke kontak domain saat perlindungan privasi diaktifkan

Jika perlindungan privasi diaktifkan untuk domain, informasi kontak untuk pendaftar, kontak teknis, dan administratif diganti dengan informasi kontak untuk layanan privasi Amazon Registrar. Misalnya, jika domain example.com terdaftar di Amazon Registrar dan jika perlindungan privasi diaktifkan, nilai Email Pendaftar dalam menanggapi kueri WHOIS akan serupa dengan owner1234@example.com.identity-protect.org.

Untuk menghubungi satu atau beberapa kontak domain saat perlindungan privasi diaktifkan, kirim email ke alamat email yang sesuai. Kami secara otomatis meneruskan email Anda ke kontak yang berlaku.

Melaporkan penyalahgunaan

Untuk melaporkan aktivitas ilegal atau pelanggaran [Kebijakan Penggunaan yang Dapat Diterima](#), termasuk konten yang tidak pantas, phishing, malware, atau spam, kirim email ke trustandsafety@support.aws.com.

Untuk melihat informasi tentang domain yang terdaftar di Route 53

1. Di browser web, buka salah satu situs web berikut:
 - [Amazon Registrar WHOIS: /whois https://registrar.amazon.com](https://registrar.amazon.com/whois)
 - [Amazon Registrar RDAP: /rdap https://registrar.amazon.com](https://registrar.amazon.com/rdap)
 - Gandi WHOIS: <https://whois.gandi.net>
2. Masukkan nama domain yang ingin Anda lihat informasinya, dan pilih Cari.

Menghapus pendaftaran nama domain

Untuk sebagian besar domain tingkat atas (TLDs), Anda dapat menghapus pendaftaran jika Anda tidak lagi menginginkannya. Jika registri memungkinkan Anda untuk menghapus pendaftaran, lakukan prosedur dalam topik ini.

Perhatikan hal-hal berikut:

Biaya pendaftaran tidak dapat dikembalikan

Jika Anda menghapus pendaftaran nama domain sebelum pendaftaran dijadwalkan berakhir, AWS tidak mengembalikan biaya pendaftaran.

TLDs yang memungkinkan Anda untuk menghapus pendaftaran domain

Untuk menentukan apakah Anda dapat menghapus pendaftaran untuk domain Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#). Jika bagian untuk TLD Anda tidak menyertakan subbagian "Penghapusan pendaftaran domain", Anda dapat menghapus domain tersebut. Sebelum Anda menghapus domain, pastikan Anda telah menonaktifkan kunci domain. Untuk informasi selengkapnya tentang menonaktifkan kunci domain, lihat [DisableDomainTransferLock](#)

Bagaimana jika Anda tidak dapat menghapus pendaftaran domain?

Jika registri untuk domain Anda tidak mengizinkan Anda untuk menghapus pendaftaran nama domain, Anda harus menunggu domain tersebut kedaluwarsa. Untuk memastikan bahwa domain tidak diperpanjang secara otomatis, nonaktifkan perpanjangan otomatis untuk domain. Ketika tanggal Kedaluwarsa lewat, Route 53 secara otomatis menghapus pendaftaran untuk domain tersebut. Untuk informasi tentang cara mengubah pengaturan pembaruan otomatis, lihat [Mengaktifkan atau menonaktifkan perpanjangan otomatis untuk domain](#).

Tunda sebelum domain dihapus dan tersedia untuk mendaftar kembali

Hampir semua registri mencegah siapa pun segera mendaftarkan domain yang baru saja kedaluwarsa. Penundaan tipikal adalah satu hingga tiga bulan, tergantung TLD. Untuk informasi selengkapnya, lihat bagian "Batas waktu untuk memperbarui dan memulihkan domain" untuk TLD Anda di [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Important

Jangan menghapus domain dan berharap untuk mendaftarkannya kembali jika Anda hanya ingin mentransfer domain antar AWS akun atau mentransfer domain ke registrar lain. Lihat dokumentasi yang berlaku sebagai gantinya:

- [Mentransfer domain ke akun lain AWS](#)
- [Mentransfer domain dari Amazon Route 53 ke registrar lain](#)

Untuk menghapus pendaftaran nama domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Domain terdaftar.
3. Pilih nama domain Anda.

Jika Anda ingin menghapus domain.co.uk, .me.uk, .org.uk, atau .uk, lihat. [Untuk menghapus pendaftaran nama domain.co.uk, .me.uk, .org.uk, dan .uk](#)

4. Jika registri untuk TLD Anda memungkinkan penghapusan pendaftaran nama domain, pilih Hapus domain.

Beberapa domain mungkin mengharuskan kami mengirim email ke pendaftar untuk domain untuk memverifikasi bahwa pendaftar ingin menghapus domain. Jika Anda menerima email, itu akan dari salah satu alamat email berikut:

- `noreply@registrar.amazon` - untuk TLDs didaftarkan oleh Amazon Registrar.
- `noreply@domainnameverification.net` atau `noreply@emailverification.info` — untuk TLDs didaftarkan oleh rekanan registrar kami, Gandi.

Untuk menentukan registrar TLD Anda, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

5. Jika Anda menerima email verifikasi, pilih tautan di email, dan setuju atau tolak permintaan untuk menghapus domain.

 Important

Kontak pendaftar harus segera mengikuti instruksi dalam email, atau kami harus membatalkan permintaan penghapusan segera setelah satu hari, seperti yang dipersyaratkan oleh ICANN.

Anda akan menerima email lain bila domain telah dihapus. Untuk menentukan status permintaan saat ini, lihat [Melihat status pendaftaran domain](#).

6. Hapus catatan di zona yang di-hosting untuk domain yang dihapus, lalu hapus zona yang di-hosting. Setelah Anda menghapus zona yang di-hosting, Route 53 berhenti menagih Anda biaya bulanan untuk zona yang di-hosting. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:
 - [Menghapus catatan](#)
 - [Menghapus zona yang di-hosting publik](#)
 - [Harga Route 53](#)
7. Jika mengalami masalah saat menghapus pendaftaran nama domain, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Untuk menghapus pendaftaran nama domain.co.uk, .me.uk, .org.uk, dan .uk

Jika Anda ingin menghapus domain.co.uk, .me.uk, .org.uk, atau .uk, Anda membuat akun dengan Nominet, registri untuk domain.uk. Untuk informasi lebih lanjut, lihat "Membatalkan nama domain Anda" di situs web Nominet, <https://www.nominet.uk/domain-support/>.

 Important

Jika Anda menghapus (membatalkan) nama domain.uk, nama domain.uk akan dihapus dalam beberapa hari dan tersedia bagi siapa saja untuk mendaftar. Jika anda hanya ingin memindahkan domain, jangan menghapusnya.

Berikut adalah gambaran umum prosesnya:

1. Di situs web Nominet, ikuti petunjuk masuk untuk pertama kalinya. Lihat <https://secure.nominet.org.uk/auth/login.html>. Nominet mengirimkan email dengan petunjuk untuk membuat kata sandi.
2. Ikuti instruksi di email yang Anda terima dari Nominet.
3. Masuk ke situs web Nominet, dan ikuti petunjuk untuk membatalkan (menghapus) nama domain.

Menghubungi AWS Support tentang masalah pendaftaran domain

AWS menyediakan paket dukungan Dasar, gratis, untuk semua AWS pelanggan. Paket tersebut mencakup bantuan untuk masalah berikut yang terkait dengan pendaftaran domain:

- Mentransfer domain ke atau dari Amazon Route 53
- Mentransfer domain antar akun AWS
- Meningkatkan kuota pada entitas Route 53, seperti jumlah domain yang dapat Anda daftarkan (Lihat [Kuota](#).)
- Mengubah pemilik domain
- Mengubah informasi kontak untuk pemilik domain
- Mengirim ulang email konfirmasi dan otorisasi
- Memperbarui domain
- Memulihkan domain yang kedaluwarsa
- Mendapatkan informasi tentang penagihan Route 53

- Memberikan bukti identitas untuk domain .uk
- Menghapus domain atau menonaktifkan perpanjangan otomatis setelah Anda menutup akun AWS

Untuk menghubungi AWS Support tentang masalah ini dan masalah lain yang terkait dengan pendaftaran domain, lakukan prosedur yang berlaku.

Topik

- [Menghubungi AWS Support ketika Anda dapat masuk ke AWS akun Anda](#)
- [Menghubungi AWS Support jika Anda tidak dapat masuk ke AWS akun](#)

Menghubungi AWS Support ketika Anda dapat masuk ke AWS akun Anda

Untuk menghubungi AWS Support ketika Anda dapat masuk ke AWS akun Anda, lakukan prosedur berikut:

1. Dengan menggunakan AWS akun tempat domain saat ini terdaftar, masuk ke [AWS Support](#).

Important

Anda harus masuk dengan menggunakan akun root tempat domain saat ini terdaftar. Persyaratan ini mencegah pengguna yang tidak sah membajak akun Anda.

2. Pilih Akun dan Penagihan
3. Tentukan nilai-nilai berikut ini:

Mengenai

Terima nilai default Dukungan Akun dan Penagihan.

Layanan

Terima nilai default Domain.

Kategori

Terima nilai default Masalah Pendaftaran.

Kepelikan

Pilih tingkat keparahan yang berlaku.

Subjek

Masukkan ringkasan singkat dari masalah ini.

Deskripsi

Jelaskan masalah yang Anda alami secara lebih mendetail, dan lampirkan dokumen atau tangkapan layar yang relevan.

Metode kontak

Pilih metode kontak, Web. Kami akan menghubungi Anda menggunakan alamat email yang terkait dengan AWS akun Anda.

4. Pilih Kirim.

Menghubungi AWS Support jika Anda tidak dapat masuk ke AWS akun

Untuk menghubungi AWS Support jika Anda tidak dapat masuk ke AWS akun, lakukan prosedur berikut:

1. Buka halaman [Saya seorang AWS pelanggan dan saya sedang mencari halaman penagihan atau dukungan akun](#).
2. Isi formulirnya.
3. Pilih Kirim.

Mengunduh laporan penagihan domain

Jika Anda mengelola beberapa domain dan ingin melihat tagihan menurut domain untuk jangka waktu tertentu, Anda dapat mengunduh laporan penagihan domain. Laporan ini mencakup semua biaya yang berlaku untuk pendaftaran domain, termasuk yang berikut:

- Mendaftarkan domain
- Memperbarui pendaftaran untuk domain
- Mentransfer domain ke Amazon Route 53
- Mengubah pemilik domain (untuk beberapa TLDs, operasi ini gratis)

Terkadang laporan penagihan Anda dapat menunjukkan periode penagihan di masa mendatang. Ini terjadi karena proses perpanjangan otomatis domain dimulai sebulan sebelum domain kedaluwarsa. Oleh karena itu, misalnya, dalam laporan Agustus Anda, Anda mungkin melihat periode penagihan yang dimulai pada bulan September setelahnya dan berjalan hingga September tahun berikutnya.

Saat menjalankan laporan menggunakan konsol, Anda dapat memilih opsi berikut:

- 12 bulan terakhir: Laporan termasuk biaya dari satu tahun sebelum Anda menjalankan laporan sampai hari ini. Misalnya, jika Anda menjalankan laporan pada 3 Juni, itu termasuk biaya dari 3 Juni tahun sebelumnya hingga hari ini.
- Bulan-bulan individu dalam setahun terakhir: Laporan mencakup biaya untuk bulan yang ditentukan.

Jika Anda menjalankan laporan secara terprogram, Anda bisa mendapatkan tagihan untuk rentang tanggal apa pun, mulai 31 Juli 2014. Itulah tanggal Route 53 mulai mendukung pendaftaran domain. Sebagai contoh, lihat [lihat penagihan](#) di Segarkan Perintah AWS CLI .

Laporan penagihan dalam format CSV, dan isinya dijelaskan oleh API. [ViewBilling](#)

Untuk mengunduh laporan penagihan domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Registered Domains (Domain terdaftar).
3. Pilih Domain billing report (Laporan penagihan domain).
4. Pilih rentang tanggal untuk laporan, lalu pilih Download domain report (Unduh laporan domain).
5. Ikuti petunjuk untuk membuka laporan atau menyimpannya.
6. Jika mengalami masalah saat mengunduh laporan penagihan domain, Anda dapat menghubungi AWS Support secara gratis. Lihat informasi yang lebih lengkap di [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Domain yang dapat Anda daftarkan dengan Amazon Route 53

Important

Pembatasan domain tingkat atas di bawah ini hanya berlaku untuk pendaftaran domain. Anda dapat menggunakan layanan DNS Route 53 dengan domain tingkat atas apa pun yang Anda

pilih dan dengan registrar domain apa pun. Informasi di halaman ini hanya berkaitan dengan domain yang dapat Anda daftarkan dengan Route 53. Untuk informasi selengkapnya tentang Route 53 sebagai layanan DNS, lihat [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#).

Daftar domain tingkat atas generik dan geografis berikut menunjukkan domain tingkat atas (TLDs) yang dapat Anda gunakan untuk mendaftarkan domain dengan Amazon Route 53.

Mendaftarkan domain dengan Route 53

Registri TLD telah menetapkan harga khusus atau premium untuk beberapa nama domain. Anda tidak dapat menggunakan Route 53 untuk mendaftarkan domain yang memiliki harga khusus atau premium. TLDs yang dapat Anda daftarkan dengan Route 53 termasuk dalam daftar berikut. Jika TLD tidak disertakan, Anda tidak dapat mendaftarkan domain dengan Route 53.

Mentransfer domain ke Route 53

Anda dapat mentransfer domain ke Route 53 jika TLD disertakan dalam daftar berikut. Jika TLD tidak disertakan, Anda tidak dapat mentransfer domain ke Route 53.

Untuk sebagian besar TLDs, Anda perlu mendapatkan kode otorisasi dari registrar saat ini untuk mentransfer domain. Untuk menentukan apakah Anda memerlukan kode otorisasi, lihat bagian “Kode otorisasi yang diperlukan untuk transfer” untuk TLD Anda.

Harga untuk pendaftaran dan transfer domain

Untuk informasi tentang biaya pendaftaran atau transfer domain ke Route 53, lihat [Harga Amazon Route 53 untuk Pendaftaran Domain](#).

Menggunakan Route 53 sebagai layanan DNS Anda

Anda dapat menggunakan Route 53 sebagai layanan DNS untuk domain apa pun, bahkan jika TLD untuk domain tidak disertakan dalam daftar berikut. Untuk informasi selengkapnya tentang Route 53 sebagai layanan DNS, lihat [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#). Untuk informasi tentang cara mentransfer layanan DNS untuk domain Anda ke Route 53, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Nama domain yang diinternasionalisasi

Tidak semua TLDs mendukung nama domain internasional (IDNs), yang berarti nama domain yang menyertakan karakter selain karakter ASCII a-z, 0-9, dan - (tanda hubung). Daftar untuk

setiap TLD menunjukkan apakah TLD itu mendukung IDNs Untuk informasi selengkapnya tentang nama domain yang diinternasionalisasi, lihat [Format nama domain DNS](#).

Mendaftarkan domain geografis dengan TLDs

Aturan untuk pendaftaran geografis TLDs bervariasi menurut negara. Beberapa negara tidak dibatasi, yang berarti bahwa siapa pun di dunia dapat mendaftar, sementara negara lain memiliki batasan tertentu, seperti residensi. Daftar untuk setiap TLD geografis menunjukkan adanya pembatasan.

Indeks untuk domain tingkat atas yang didukung

Topik

- [Domain tingkat atas generik](#)
- [Domain tingkat atas geografis](#)

Domain tingkat atas generik

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [WXYZ](#)

A

[.ac](#), [.academy](#), [.accountants](#), [.aktor](#), [.adult](#), [.agency](#), [.angkatan udara](#), [.apartments](#), [.associates](#),
[.auction](#), [.audio](#)

B

[.band](#), [.bargains](#), [.bir](#), [.bertaruh](#), [.tawaran](#), [.bike](#), [.bingo](#), [.bio](#), [.biz](#), [.black](#), [.blue](#), [.bot](#), [.boutique](#),
[.builders](#), [.business](#), [.buzz](#)

C

[.cab](#), [.cafe](#), [.camera](#), [.camp](#), [.capital](#), [.cards](#), [.care](#), [.careers](#), [.cash](#), [.casino](#), [.catering](#), [.cc](#), [.center](#),
[.ceo](#), [.chat](#), [.cheap](#), [.natal](#), [.church](#), [.city](#), [.claims](#), [.cleaning](#), [.click](#), [.clinic](#), [.clothing](#), [.cloud](#), [.club](#),
[.coach](#), [.codes](#), [.coffee](#), [.college](#), [.com](#), [.community](#), [.company](#), [.computer](#), [.condos](#), [.construction](#),
[.consulting](#), [.kontak](#), [.contractors](#), [.cool](#), [.coupons](#), [.credit](#), [.creditcard](#), [.cruises](#)

D

[.dance](#), [.dating](#), [.kesepakatan](#), [.deals](#), [.derajat](#), [.delivery](#), [.democrat](#), [.dental](#), [.desain](#), [.diamond](#),
[.diet](#), [.digital](#), [.direct](#), [.directory](#), [.discount](#), [.dog](#), [.domains](#)

E

[.education](#), [.email](#), [.energy](#), [.engineering](#), [.enterprises](#), [.equipment](#), [.estate](#), [.events](#), [.exchange](#),
[.expert](#), [.exposed](#), [.express](#)

F

[.fail](#), [.penggemar](#), [.farm](#), [.finance](#), [.financial](#), [.fish](#), [.fitness](#), [.flights](#), [.florist](#), [.flowers](#), [.fm](#), [.football](#),
[.forsale](#), [.foundation](#), [.gratis](#), [.menyenangkan](#), [.fund](#), [.furniture](#), [.futbol](#), [.fyi](#)

G

[.gallery](#), [.permainan](#), [.gift](#), [.gifts](#), [.memberikan](#), [.glass](#), [.global](#), [.gmbh](#), [.gold](#), [.golf](#), [.graphics](#), [.gratis](#),
[.green](#), [.gripe](#), [.kelompok](#), [.guide](#), [.guitars](#), [.guru](#)

H

[.haus](#), [.healthcare](#), [.help](#), [.hiv](#), [.hockey](#), [.holdings](#), [.holiday](#), [.host](#), [.hosting](#), [.panas](#), [.house](#)

I

[.im](#), [.immo](#), [.immobilien](#), [.industries](#), [.info](#), [.ink](#), [.institute](#), [.insure](#), [.international](#), [.investments](#), [.io](#),
[.irish](#)

J

[.jewelry](#), [.juegos](#)

K

[.kaufen](#), [.kim](#), [.kitchen](#), [.kiwi](#)

L

[.land](#), [.hukum](#), [.lease](#), [.legal](#), [.lgbt](#), [.life](#), [.lighting](#), [.limited](#), [.limo](#), [.link](#), [.live](#), [.llc](#), [.loan](#), [.loans](#), [.lol](#), [.ltd](#)

M

[.maison](#), [.management](#), [.marketing](#), [.mba](#), [.media](#), [.memorial](#), [.mobi](#), [.moda](#), [.moi](#), [.money](#),
[.mortgage](#), [.movie](#)

N

[.name](#), [.net](#), [.network](#), [.news](#), [.ninja](#), [.sekarang](#)

O

[.onl](#), [.online](#), [.org](#)

P

[.partners](#), [.parts](#), [.photo](#), [.photography](#), [.photos](#), [.pics](#), [.pictures](#), [.pink](#), [.pizza](#), [.place](#), [.plumbing](#), [.plus](#), [.poker](#), [.porno](#), [.tekan](#), [.pro](#), [.productions](#), [.properties](#), [.property](#), [.pub](#), [.pw \(Palau\)](#)

Q

[.qpon](#)

R

[.recipes](#), [.red](#), [.reise](#), [.reisen](#), [.rentals](#), [.repair](#), [.report](#), [.republican](#), [.restaurant](#), [.reviews](#), [.rip](#), [.rocks](#), [.run](#)

S

[.sale](#), [.sarl](#), [.school](#), [.schule](#), [.services](#), [.sex](#), [.sexy](#), [.shiksha](#), [.shoes](#), [.toko](#), [.belanja](#), [.show](#), [.singles](#), [.situs](#), [.ski](#), [.soccer](#), [.social](#), [.solar](#), [.solutions](#), [.perangkat lunak](#), [.ruang](#), [.tempat](#), [.toko](#), [.aliran](#), [.studio](#), [.style](#), [.sucks](#), [.supplies](#), [.supply](#), [.support](#), [.surgery](#), [.systems](#)

T

[.tattoo](#), [.tax](#), [.taxi](#), [.team](#), [.tech](#), [.technology](#), [.tennis](#), [.theater](#), [.tienda](#), [.tips](#), [.tires](#), [.today](#), [.tools](#), [.tours](#), [.town](#), [.toys](#), [.trade](#), [.training](#), [.tv](#)

U

[.university](#), [.uno](#)

V

[.vacations](#), [.vegas](#), [.ventures](#), [.vg](#), [.viajes](#), [.video](#), [.villa](#), [.vision](#), [.suara](#), [.voyage](#)

WXYZ

[.watch](#), [.website](#), [.pernikahan](#), [.wiki](#), [.anggur](#), [.kerja](#), [.works](#), [.world](#), [.wtf](#), [.xxx](#), [.xyz](#), [.zone](#)

Domain tingkat atas geografis

Afrika

[.ac \(Pulau Ascension\)](#), [.co.za \(Afrika Selatan\)](#), [.sh \(Saint Helena\)](#)

Amerika

[.ai \(Anguila\)](#), [.ca \(Kanada\)](#), [.cl \(Chili\)](#), [.co \(Kolombia\)](#), [.com.ar \(Argentina\)](#), [.com.br \(Brasil\)](#), [.com.mx \(Meksiko\)](#), [.mx \(Meksiko\)](#), [.us \(Amerika Serikat\)](#), [.vc \(Saint Vincent dan Grenadines\)](#), [.vg \(Kepulauan Virgin Inggris\)](#)

Asia/Oseania

[.au \(Australia\)](#), [.cc \(Pulau Cocos \(Keeling\)\)](#), [.co.nz \(Selandia Baru\)](#), [.com.au \(Australia\)](#), [.com.sg \(Republik Singapura\)](#), [.fm \(Negara Federasi Mikronesia\)](#), [.in \(India\)](#), [.jp \(Jepang\)](#), [.io \(Wilayah Samudra Hindia Britania\)](#), [.net.au \(Australia\)](#), [.net.nz \(Selandia Baru\)](#), [.nz \(Selandia Baru\)](#), [.org.nz \(Selandia Baru\)](#), [.pw \(Palau\)](#), [.qa \(Qatar\)](#), [.ru \(Federasi Rusia\)](#), [.sg \(Republik Singapura\)](#)

Eropa

[.be \(Belgia\)](#), [.berlin \(kota Berlin di Jerman\)](#), [.ch \(Swiss\)](#), [.co.uk \(Inggris Raya\)](#), [.cz \(Republik Ceko\)](#), [.de \(Jerman\)](#), [.es \(Spanyol\)](#), [.eu \(Uni Eropa\)](#), [.fi \(Finlandia\)](#), [.fr \(Prancis\)](#), [.gg \(Guernsey\)](#), [.im \(Pulau Man\)](#), [.it \(Italia\)](#), [.me \(Montenegro\)](#), [.me.uk \(Inggris Raya\)](#), [.nl \(Belanda\)](#), [.org.uk \(Inggris Raya\)](#), [.ruhr \(wilayah Ruhr, bagian barat Jerman\)](#), [.se \(Swedia\)](#), [.uk \(Inggris Raya\)](#), [.wien \(kota Wina di Austria\)](#)

Domain tingkat atas generik

Domain tingkat atas generik (gTLDs) adalah ekstensi global yang digunakan dan diakui di seluruh dunia, seperti [.com](#), [.net](#), dan [.org](#). Juga termasuk domain khusus seperti [.bike](#), [.condos](#), dan [.marketing](#).

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [WXYZ](#)

A

[.ac](#), [.academy](#), [.accountants](#), [.aktor](#), [.adult](#), [.agency](#), [.angkatan udara](#), [.apartments](#), [.associates](#), [.auction](#), [.audio](#)

B

[.band](#), [.bargains](#), [.bir](#), [.bertaruh](#), [.tawaran](#), [.bike](#), [.bingo](#), [.bio](#), [.biz](#), [.black](#), [.blue](#), [.bot](#), [.boutique](#), [.builders](#), [.business](#), [.buzz](#)

C

[.cab](#), [.cafe](#), [.camera](#), [.camp](#), [.capital](#), [.cards](#), [.care](#), [.careers](#), [.cash](#), [.casino](#), [.catering](#), [.cc](#), [.center](#), [.ceo](#), [.chat](#), [.cheap](#), [.church](#), [.natal](#), [.city](#), [.claims](#), [.cleaning](#), [.click](#), [.clinic](#), [.clothing](#), [.cloud](#), [.club](#),

[.coach](#), [.codes](#), [.coffee](#), [.college](#), [.com](#), [.community](#), [.company](#), [.computer](#), [.condos](#), [.construction](#),
[.consulting](#), [.kontak](#), [.contractors](#), [.cool](#), [.coupons](#), [.credit](#), [.creditcard](#), [.cruises](#)

D

[.dance](#), [.dating](#), [.kesepakatan](#), [.deals](#), [.derajat](#), [.delivery](#), [.democrat](#), [.dental](#), [.desain](#), [.diamond](#),
[.diet](#), [.digital](#), [.direct](#), [.directory](#), [.discount](#), [.dog](#), [.domains](#)

E

[.education](#), [.email](#), [.energy](#), [.engineering](#), [.enterprises](#), [.equipment](#), [.estate](#), [.events](#), [.exchange](#),
[.expert](#), [.exposed](#), [.express](#)

F

[.fail](#), [.penggemar](#), [.farm](#), [.finance](#), [.financial](#), [.fish](#), [.fitness](#), [.flights](#), [.florist](#), [.flowers](#), [.fm](#), [.football](#),
[.forsale](#), [.foundation](#), [.gratis](#), [.menyenangkan](#), [.fund](#), [.furniture](#), [.futbol](#), [.fyi](#)

G

[.gallery](#), [.permainan](#), [.gift](#), [.gifts](#), [.memberikan](#), [.glass](#), [.global](#), [.gmbh](#), [.gold](#), [.golf](#), [.graphics](#), [.gratis](#),
[.green](#), [.gripe](#), [.kelompok](#), [.guide](#), [.guitars](#), [.guru](#)

H

[.haus](#), [.healthcare](#), [.help](#), [.hiv](#), [.hockey](#), [.holdings](#), [.holiday](#), [.host](#), [.hosting](#), [.panas](#), [.house](#)

I

[.im](#), [.immo](#), [.immobilien](#), [.industries](#), [.info](#), [.ink](#), [.institute](#), [.insure](#), [.international](#), [.investments](#), [.io](#),
[.irish](#)

J

[.jewelry](#), [.juegos](#)

K

[.kaufen](#), [.kim](#), [.kitchen](#), [.kiwi](#)

L

[.land](#), [.hukum](#), [.lease](#), [.legal](#), [.lgbt](#), [.life](#), [.lighting](#), [.limited](#), [.limo](#), [.link](#), [.live](#), [.llc](#), [.loan](#), [.loans](#), [.lol](#), [.ltd](#)

M

[.maison](#), [.management](#), [.marketing](#), [.mba](#), [.media](#), [.memorial](#), [.mobi](#), [.moda](#), [.moi](#), [.money](#),
[.mortgage](#), [.movie](#)

N

[.name](#), [.net](#), [.network](#), [.news](#), [.ninja](#), [.sekarang](#)

O

[.onl](#), [.online](#), [.org](#)

P

[.partners](#), [.parts](#), [.photo](#), [.photography](#), [.photos](#), [.pics](#), [.pictures](#), [.pink](#), [.pizza](#), [.place](#), [.plumbing](#),
[.plus](#), [.poker](#), [.porno](#), [.tekan](#), [.pro](#), [.productions](#), [.properties](#), [.property](#), [.pub](#)

Q

[.qpon](#)

R

[.recipes](#), [.red](#), [.reise](#), [.reisen](#), [.rentals](#), [.repair](#), [.report](#), [.republican](#), [.restaurant](#), [.reviews](#), [.rip](#), [.rocks](#),
[.run](#)

S

[.sale](#), [.sarl](#), [.school](#), [.schule](#), [.services](#), [.sex](#), [.sexy](#), [.shiksha](#), [.shoes](#), [.toko](#), [.belanja](#), [.show](#),
[.singles](#), [.situs](#), [.ski](#), [.soccer](#), [.social](#), [.solar](#), [.solutions](#), [.perangkat lunak](#), [.ruang](#), [.tempat](#), [.toko](#),
[.aliran](#), [.studio](#), [.style](#), [.sucks](#), [.supplies](#), [.supply](#), [.support](#), [.surgery](#), [.systems](#)

T

[.tattoo](#), [.tax](#), [.taxi](#), [.team](#), [.tech](#), [.technology](#), [.tennis](#), [.theater](#), [.tienda](#), [.tips](#), [.tires](#), [.today](#), [.tools](#),
[.tours](#), [.town](#), [.toys](#), [.trade](#), [.training](#), [.tv](#)

U

[.university](#), [.uno](#)

V

[.vacations](#), [.vegas](#), [.ventures](#), [.vg](#), [.viajes](#), [.video](#), [.villa](#), [.vision](#), [.suara](#), [.voyage](#)

WXYZ

[.watch](#), [.website](#), [.pernikahan](#), [.wiki](#), [.anggur](#), [.kerja](#), [.works](#), [.world](#), [.wtf](#), [.xxx](#), [.xyz](#), [.zone](#)

.ac

Lihat [.ac \(Pulau Ascension\)](#).

[Return to index](#)

.academy

Digunakan oleh lembaga pendidikan seperti sekolah dan universitas. Juga digunakan oleh perekrut, penasihat, pengiklan, siswa, guru, dan administrator yang berafiliasi dengan lembaga pendidikan.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.accountants

Digunakan oleh bisnis, grup, dan individu yang berafiliasi dengan profesi akuntansi.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.aktor

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.adult

Digunakan untuk situs web yang meng-host konten khusus dewasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.agency

Digunakan oleh bisnis atau grup yang mengidentifikasi dirinya sebagai lembaga.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.angkatan udara

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.apartments

Digunakan oleh agen real estat, pemilik properti yang disewakan, dan penyewa.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.associates

Digunakan oleh bisnis dan firma yang menggunakan istilah "rekanan" dalam nama mereka. Juga digunakan oleh grup atau lembaga yang ingin menunjukkan sifat profesional organisasi mereka.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.auction

Digunakan untuk acara yang berkaitan dengan lelang serta pembelian dan penjualan berbasis lelang.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Spanyol, dan Latin.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa

- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.audio

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .audio baru atau mentransfer domain .audio ke Route 53. Kami akan terus mendukung domain .audio yang sudah terdaftar dengan Route 53.

Digunakan oleh industri audiovisual dan siapa saja yang tertarik pada penyiaran, peralatan suara, produksi audio, dan streaming audio.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .audio ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.band

Digunakan untuk berbagi informasi tentang band musik dan acara band. Juga digunakan oleh musisi untuk terhubung dengan basis penggemar mereka dan menjual merchandise yang berhubungan dengan band.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Spanyol, dan Latin.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bargains

Digunakan untuk informasi tentang penjualan dan promosi.

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa

- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bir

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bertaruh

[Return to index](#)

Masa sewa untuk pendaftaran dan pembaruan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tawaran

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bike

Digunakan oleh perusahaan atau grup yang melayani pengendara sepeda, seperti toko sepeda, dealer sepeda motor, dan bengkel.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bingo

Digunakan untuk situs game online atau untuk berbagi informasi tentang permainan bingo.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bio

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.biz

Digunakan untuk bisnis atau penggunaan komersial.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa Sederhana, Tionghoa Tradisional, Denmark, Finlandia, Jerman, Hungaria, Jepang, Korea, Latvia, Lithuania, Norwegia, Polandia, Portugis, Spanyol, dan Swedia.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.black

Digunakan oleh mereka yang suka warna hitam atau mereka yang ingin mengasosiasikan warna hitam dengan bisnis atau merek mereka.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.blue

Digunakan oleh mereka yang suka warna biru atau mereka yang ingin mengasosiasikan warna biru dengan bisnis atau merek mereka.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.bot

Digunakan untuk chatbot dan produk dan layanan terkait AI. Ekstensi domain ini membantu menyampaikan sifat sistem otomatis, antarmuka percakapan, dan teknologi yang muncul dalam kecerdasan buatan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.boutique

Digunakan untuk informasi tentang butik dan toko-toko khusus berskala kecil.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.builders

Digunakan oleh perusahaan dan individu yang berafiliasi dengan industri konstruksi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.business

Digunakan oleh segala jenis bisnis. Dapat digunakan sebagai alternatif ekstensi .biz.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.buzz

Digunakan untuk informasi tentang berita dan acara terbaru.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cab

Digunakan oleh perusahaan dan individu yang berafiliasi dengan industri angkutan taksi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cafe

Digunakan oleh bisnis kafe dan mereka yang memiliki minat dalam budaya kafe.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.camera

Digunakan oleh penggemar fotografi dan siapa saja yang ingin berbagi foto.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.camp

Digunakan oleh dinas pertamanan dan rekreasi, kamp musim panas, lokakarya penulis, kamp kebugaran, dan penggemar berkemah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.capital

Digunakan sebagai kategori umum yang menjelaskan segala jenis modal/ibu kota (capital), seperti modal keuangan atau ibu kota dari sebuah kota.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cards

Digunakan oleh bisnis yang mengkhususkan diri pada kartu seperti kartu elektronik, kartu ucapan cetak, kartu nama, dan kartu remi. Juga ideal untuk pemain yang ingin membahas aturan dan strategi permainan kartu.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.care

Digunakan oleh bisnis atau lembaga di bidang jasa perawatan. Juga digunakan oleh organisasi amal.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.careers

Digunakan untuk informasi tentang perekrutan pekerjaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cash

Digunakan oleh organisasi, kelompok, atau individu yang terlibat dalam kegiatan yang berhubungan dengan uang.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.casino

Digunakan oleh industri perjudian atau oleh pemain yang ingin berbagi informasi tentang permainan judi dan kasino.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.catering

Digunakan oleh bisnis katering atau mereka yang berbagi informasi tentang acara terkait makanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cc

Lihat [.cc \(Pulau Cocos \(Keeling\)\)](#).

[Return to index](#)

.center

Digunakan sebagai ekstensi generik untuk segala sesuatu mulai dari organisasi penelitian hingga pusat komunitas.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ceo

Digunakan untuk informasi tentang CEOs dan sederajat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Jerman.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.chat

Digunakan oleh segala jenis situs web obrolan online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cheap

Digunakan oleh situs web perdagangan elektronik untuk mempromosikan dan menjual produk murah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.natal

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Perpanjangan terlambat dengan Route 53 dimungkinkan: Hingga 43 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 44 hari setelah kedaluwarsa

- Pemulihan dengan registri dimungkinkan: Antara 44 hari dan 86 hari setelah kedaluwarsa
- Domain dihapus dari registri: 86 hari setelah kedaluwarsa

.church

Digunakan oleh gereja dengan berbagai ukuran atau denominasi untuk terhubung dengan jemaat mereka serta untuk memublikasikan informasi tentang acara dan kegiatan yang berhubungan dengan gereja.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.city

Digunakan untuk memberikan informasi tentang kota tertentu, seperti tempat menarik, area lokal terbaik untuk dikunjungi, atau kegiatan lingkungan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.claims

Digunakan oleh perusahaan yang menangani klaim asuransi atau memberikan layanan hukum.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cleaning

Digunakan oleh bisnis atau individu yang menyediakan layanan pembersihan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.click

Digunakan oleh bisnis yang ingin mengasosiasikan tindakan mengklik dengan situs web mereka, misalnya, mengklik produk di situs web untuk membelinya.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.clinic

Digunakan oleh industri perawatan kesehatan dan oleh profesional medis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.clothing

Digunakan oleh orang-orang di industri fashion, termasuk pengecer, department store, desainer, penjahit, dan outlet.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cloud

Digunakan sebagai ekstensi umum, namun ideal untuk perusahaan yang menyediakan teknologi dan layanan komputasi cloud.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.club

Digunakan oleh semua jenis klub atau organisasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Spanyol dan Jepang.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.coach

Digunakan oleh siapa saja yang tertarik dalam pelatihan, seperti profesional olahraga, pelatih gaya hidup, atau pelatih perusahaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.codes

Digunakan sebagai ekstensi generik untuk semua jenis kode, seperti kode etik, kode bangunan, atau kode pemrograman.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.coffee

Digunakan oleh orang-orang dalam industri kopi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.college

Digunakan oleh lembaga pendidikan seperti sekolah dan universitas. Juga digunakan oleh perekrut, penasihat, pengiklan, siswa, guru, dan administrator yang berafiliasi dengan lembaga pendidikan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Tionghoa sederhana serta tradisional, Sirilik, Yunani, Ibrani, Jepang, dan Thailand.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.com

Digunakan untuk situs web komersial. Ini adalah ekstensi paling populer di internet.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.community

Digunakan oleh semua jenis komunitas, klub, organisasi, atau kelompok dengan minat khusus.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.company

Digunakan sebagai ekstensi generik untuk semua jenis perusahaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.computer

Digunakan sebagai ekstensi generik untuk informasi tentang komputer.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.condos

Digunakan oleh individu dan bisnis yang berkaitan dengan kondominium.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.construction

Digunakan oleh mereka dalam industri konstruksi, seperti pembuat bangunan dan kontraktor.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.consulting

Digunakan oleh konsultan dan orang lain yang berafiliasi dengan industri konsultasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Tionghoa, Prancis, Sirilik, Devanagari, Jerman, Yunani, Ibrani, Jepang, Korea, Latin, Spanyol, Tamil, dan Thailand.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kontak

Digunakan oleh gereja dengan berbagai ukuran atau denominasi untuk terhubung dengan jemaat mereka serta untuk memublikasikan informasi tentang acara dan kegiatan yang berhubungan dengan gereja.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.contractors

Digunakan oleh kontraktor, seperti kontraktor dalam industri konstruksi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cool

Digunakan oleh organisasi dan kelompok yang ingin mengasosiasikan merek mereka dengan tren terbaru.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.coupons

Digunakan oleh pengecer dan produsen yang menyediakan kupon online serta kode kupon.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.credit

Digunakan oleh industri kredit.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.creditcard

Digunakan oleh perusahaan atau bank yang menerbitkan kartu kredit.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.cruises

Digunakan oleh industri pelayaran.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.dance

Digunakan oleh penari, instruktur tari, dan sekolah tari.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.dating

Digunakan untuk situs web kencan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kesepakatan

Digunakan untuk situs web yang menawarkan penawaran, diskon, dan penawaran khusus.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.deals

Digunakan untuk memberikan informasi tentang penawaran dan penjualan online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.derajat

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.delivery

Digunakan oleh perusahaan yang mengirimkan segala jenis barang dagangan atau layanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.democrat

Digunakan untuk informasi tentang Partai Demokrat (AS). Juga digunakan oleh pejabat yang mencalonkan diri sebagai kantor dewan terpilih, dewan terpilih, penggemar politik, konsultan, dan penasihat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.dental

Digunakan oleh profesional kesehatan gigi dan pemasok peralatan kesehatan gigi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.desain

Digunakan oleh gereja dengan berbagai ukuran atau denominasi untuk terhubung dengan jemaat mereka serta untuk memublikasikan informasi tentang acara dan kegiatan yang berhubungan dengan gereja.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.diamond

Digunakan oleh penggemar berlian dan orang-orang dalam industri berlian, termasuk penjual, reseller, dan pembuat merchandise.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.diet

 Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .diet baru atau mentransfer domain .diet ke Route 53. Kami akan terus mendukung domain .diet yang sudah terdaftar dengan Route 53.

Digunakan oleh profesional kesehatan dan kebugaran.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .dit ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.digital

Digunakan untuk semua hal yang berkaitan dengan dunia digital, tetapi ideal untuk bisnis teknologi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.direct

Digunakan sebagai ekstensi umum, namun ideal bagi mereka yang menjual produk langsung ke pelanggan melalui situs web perdagangan elektronik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.directory

Digunakan oleh sektor media.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.discount

Digunakan untuk situs web diskon dan bisnis yang memangkas harga.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.dog

Digunakan oleh pecinta anjing serta mereka yang menyediakan layanan dan produk untuk anjing.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.domains

Digunakan untuk informasi tentang nama domain.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.education

Digunakan untuk informasi tentang pendidikan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.email

Digunakan untuk informasi tentang mempromosikan email.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.energy

Digunakan sebagai ekstensi umum, namun ideal bagi mereka yang berada di bidang energi atau konservasi energi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.engineering

Digunakan oleh firma dan profesional di bidang teknik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.enterprises

Digunakan untuk informasi tentang perusahaan dan bisnis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.equipment

Digunakan untuk informasi tentang peralatan, pengecer atau produsen peralatan, dan toko penyewaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.estate

Digunakan untuk informasi tentang perumahan dan sektor perumahan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.events

Digunakan untuk informasi tentang semua jenis acara.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.exchange

Digunakan untuk semua jenis pertukaran: bursa saham, pertukaran barang, atau bahkan pertukaran informasi sederhana.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.expert

Digunakan oleh mereka yang memiliki pengetahuan khusus di berbagai bidang.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.exposed

Digunakan sebagai ekstensi generik untuk berbagai subjek, termasuk fotografi, tabloid, dan jurnalisme investigasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.express

Digunakan sebagai ekstensi umum, tapi ideal bagi mereka yang ingin menekankan pengiriman cepat untuk barang atau jasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.fail

Digunakan oleh siapa saja yang telah membuat kesalahan, tapi ideal untuk memublikasikan blunder dan kesalahan "gagal" yang lucu.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.penggemar

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.farm

Digunakan oleh orang-orang di industri pertanian, seperti petani dan insinyur pertanian.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.finance

Digunakan oleh sektor keuangan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.financial

Digunakan oleh sektor keuangan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.fish

Digunakan sebagai ekstensi umum, tapi ideal untuk situs web yang berhubungan dengan ikan dan memancing.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.fitness

Digunakan untuk mempromosikan kebugaran dan layanan kebugaran.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.flights

Digunakan oleh agen perjalanan, maskapai penerbangan, dan siapa saja yang berafiliasi dengan industri perjalanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.florist

Digunakan oleh toko bunga.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.flowers

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .flowers baru atau mentransfer domain .flowers ke Route 53. Kami akan terus mendukung domain .flowers yang sudah terdaftar dengan Route 53.

Digunakan untuk segala sesuatu yang berhubungan dengan bunga, seperti penjualan bunga online atau informasi tentang menanam dan memelihara bunga.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .flowers ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.fm

Lihat [.fm \(Negara Federasi Mikronesia\)](#).

[Return to index](#)

.football

Digunakan oleh siapa saja yang terlibat dalam olahraga American Football.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.forsale

Digunakan untuk menjual barang dan jasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.foundation

Digunakan oleh organisasi nirlaba, badan amal, dan jenis yayasan lainnya.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gratis

Digunakan untuk situs web yang menawarkan produk, layanan, atau konten gratis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.menyenangkan

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.fund

Digunakan sebagai ekstensi umum untuk apapun yang berhubungan dengan pendanaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.furniture

Digunakan oleh pembuat dan penjual furnitur serta siapa saja yang berafiliasi dengan industri furnitur.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.futbol

Digunakan untuk informasi tentang sepak bola.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.fyi

Digunakan sebagai ekstensi umum, tapi ideal untuk berbagi semua jenis informasi. "FYI" adalah singkatan dari "for your information" (perlu Anda ketahui).

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gallery

Digunakan oleh pemilik galeri seni.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.permainan

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gift

Digunakan oleh bisnis atau organisasi yang menjual hadiah atau menyediakan layanan yang berhubungan dengan hadiah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gifts

Digunakan oleh bisnis atau organisasi yang menjual hadiah atau menyediakan layanan yang berhubungan dengan hadiah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.memberikan

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.glass

Digunakan oleh orang-orang di industri kaca, seperti pemotong kaca dan pemasang jendela.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.global

Digunakan oleh bisnis atau grup dengan pasar atau visi internasional.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Belarusia, Bosnia, Bulgaria, Tionghoa (Sederhana), Tionghoa (Tradisional), Denmark, Jerman, Hindi, Hungaria, Islandia, Korea, Latvia, Lithuania, Macedonia, Montenegro, Polandia, Rusia, Serbia, Spanyol, Swedia, dan Ukraina.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gmbh

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gold

Digunakan sebagai ekstensi umum, namun ideal untuk perusahaan yang membeli atau menjual emas atau produk emas.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.golf

Digunakan untuk situs web yang ditujukan bagi permainan golf.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.graphics

Digunakan oleh orang-orang dalam industri grafis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gratis

Digunakan untuk situs web yang menawarkan produk gratis, seperti item promosi, unduhan, atau kupon. "Gratis" adalah kata dalam bahasa Spanyol yang berarti "tanpa biaya."

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.green

Digunakan untuk situs web yang ditujukan untuk konservasi, ekologi, lingkungan, dan gaya hidup ramah lingkungan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.gripe

Digunakan untuk berbagi keluhan dan kritik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kelompok

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.guide

Digunakan sebagai ekstensi umum, namun ideal untuk situs web yang berfokus pada tujuan, layanan, dan produk wisata.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.guitars

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .guitars baru atau mentransfer domain .guitars ke Route 53. Kami akan terus mendukung domain .guitars yang sudah terdaftar dengan Route 53.

Digunakan oleh penggemar gitar.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .guitars ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.guru

Digunakan oleh mereka yang ingin berbagi pengetahuan tentang berbagai hal.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.haus

Digunakan oleh industri real estat dan konstruksi. "Haus" adalah kata dalam bahasa Jerman yang berarti "rumah".

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.healthcare

Digunakan oleh sektor pemeliharaan kesehatan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.help

Digunakan sebagai ekstensi umum, namun ideal untuk situs web yang memberikan bantuan dan informasi online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.hiv

Digunakan untuk situs web yang ditujukan untuk memerangi HIV.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.hockey

Digunakan untuk situs web yang ditujukan bagi permainan hoki.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.holdings

Digunakan oleh penasihat keuangan, pialang saham, dan mereka yang bekerja dalam bidang investasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.holiday

Digunakan oleh mereka di industri perjalanan serta individu dan bisnis yang terlibat dalam perencanaan pesta dan acara-acara khusus.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.host

Digunakan oleh perusahaan yang menyediakan platform dan layanan hosting web.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Tionghoa Sederhana, Tionghoa Tradisional, Yunani, Ibrani, Jepang, dan Thailand.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.hosting

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .hosting baru atau mentransfer domain .hosting ke Route 53. Kami akan terus mendukung domain .hosting yang sudah terdaftar dengan Route 53.

Digunakan untuk situs web hosting atau oleh orang-orang di industri hosting.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .hosting ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.panas

Digunakan untuk situs web yang menampilkan topik tren, konten populer, atau penawaran yang sensitif terhadap waktu.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.house

Digunakan oleh agen dan pembeli real estat serta penjual rumah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.im

Lihat [.im \(Pulau Man\)](#).

[Return to index](#)

.immo

Digunakan oleh sektor real estat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.immobilien

Digunakan untuk informasi tentang real estat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.industries

Digunakan oleh bisnis atau perusahaan komersial yang ingin mengidentifikasi diri mereka sebagai industri.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.info

Digunakan untuk penyebaran informasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ink

Digunakan oleh penggemar tato atau industri apa pun yang terkait dengan tinta, seperti industri percetakan dan penerbitan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab dan Latin.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.institute

Digunakan oleh organisasi atau grup mana pun, terutama organisasi penelitian dan pendidikan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.insure

Digunakan oleh perusahaan asuransi dan broker asuransi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.international

Digunakan oleh bisnis yang memiliki rantai internasional, individu yang bepergian secara internasional, atau organisasi amal dengan pengaruh internasional.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.investments

Digunakan sebagai ekstensi umum, namun ideal untuk mempromosikan peluang investasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.io

Lihat [.io \(Wilayah Samudra Hindia Britania\)](#).

[Return to index](#)

.irish

Digunakan untuk mempromosikan budaya dan organisasi Irlandia.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Tionghoa Sederhana, Tionghoa Tradisional, Prancis, Jerman, Yunani, Ibrani, Jepang, Korea, Spanyol, Tamil, dan Thailand.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.jewelry

Digunakan oleh penjual dan pembeli perhiasan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.juegos

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .juegos baru atau mentransfer domain .juegos ke Route 53. Kami akan terus mendukung domain .juegos yang sudah terdaftar dengan Route 53.

Digunakan untuk semua jenis situs web game. "Juegos" adalah kata dalam Spanyol yang berarti "permainan."

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .juegos ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kaufen

Digunakan untuk informasi tentang perdagangan elektronik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kim

Digunakan oleh orang-orang yang memiliki nama atau nama keluarga Kim.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kitchen

Digunakan oleh pengecer peralatan dapur, juru masak, blogger makanan, dan siapa saja di industri makanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kiwi

Digunakan oleh perusahaan dan individu yang ingin mendukung budaya kiwi Selandia Baru. Ini juga digunakan sebagai platform untuk bantuan amal dalam rekonstruksi Christchurch, yang rusak akibat gempa bumi pada tahun 2010 dan 2011.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Maori.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.land

Digunakan oleh petani, agen real estat, developer komersial, dan siapa saja yang tertarik pada properti.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.hukum

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.lease

Digunakan oleh makelar, pemilik properti yang disewakan, dan penyewa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.legal

Digunakan oleh anggota profesi hukum.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.lgbt

Digunakan oleh komunitas lesbian, gay, biseksual, dan transgender.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.life

Digunakan sebagai ekstensi umum, serta cocok untuk berbagai bisnis, kelompok, dan individu.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.lighting

Digunakan oleh fotografer, desainer, arsitek, insinyur, dan lainnya yang tertarik dengan pencahayaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.limited

Digunakan sebagai ekstensi umum, serta cocok untuk berbagai bisnis, kelompok, dan individu.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.limo

Digunakan oleh sopir, perusahaan limosin, dan agen penyewaan mobil.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.link

Digunakan untuk informasi tentang pembuatan tautan pintasan online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Uniregistry adalah registri untuk domain.LINK. Karena kebijakan Uniregistry, [WHOIS](#) tingkat registri menunjukkan “REDACTED FOR PRIVACY”. Menghapus fitur perlindungan privasi kami hanya akan memengaruhi informasi yang ditampilkan di [Amazon Registrar WHOIS tingkat registrar](#).

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.live

Digunakan sebagai ekstensi umum, serta cocok untuk berbagai bisnis, kelompok, dan individu.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa

- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.llc

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.loan

Digunakan oleh pemberi pinjaman, peminjam, dan profesional dalam bidang kredit.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Denmark, Jerman, Norwegia, dan Swedia.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.loans

Digunakan oleh pemberi pinjaman, peminjam, dan profesional dalam bidang kredit.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.lol

Digunakan untuk situs web humor dan komedi. "LOL" adalah singkatan dari "laugh out loud" (tertawa terbahak-bahak).

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik, Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ltd

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.maison

Digunakan oleh sektor real estat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.management

Digunakan untuk informasi tentang dunia bisnis dan manajemen perusahaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.marketing

Digunakan oleh sektor pemasaran untuk berbagai keperluan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.mba

Digunakan untuk situs web yang memberikan informasi tentang gelar master dalam administrasi bisnis (MBA).

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.media

Digunakan oleh sektor media dan hiburan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.memorial

Digunakan oleh organisasi peringatan yang didedikasikan untuk menghormati peristiwa dan orang-orang.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.mobi

Digunakan oleh perusahaan dan individu yang ingin situs web mereka dapat diakses melalui ponsel.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.moda

Digunakan untuk informasi tentang fashion.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.moi

Bahasa Prancis untuk “aku.” Digunakan untuk memberi sinyal konten berbahasa Prancis ke pengguna akhir Francophone. Cocokkan untuk blog pribadi CVs,, portofolio, dan hobi atau situs minat dalam bahasa Prancis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.money

Digunakan untuk situs web yang berfokus pada uang dan kegiatan yang berhubungan dengan uang.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.mortgage

Digunakan oleh industri hipotek.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.movie

Digunakan untuk situs web yang memberikan informasi tentang film dan pembuatan film. Cocok untuk profesional dan penggemar.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.name

Digunakan oleh siapa saja yang ingin membuat web yang dipersonalisasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Verisign, registri untuk .name TLDs, memungkinkan Anda mendaftarkan domain tingkat kedua (nama.name) dan domain tingkat ketiga (nama depan. nama belakang .name). Route 53 hanya mendukung domain tingkat dua, baik untuk mendaftarkan domain dan mentransfer domain yang ada ke Route 53.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.net

Digunakan untuk semua jenis situs web. Ekstensi .net adalah singkatan dari network (jaringan).

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.network

Digunakan oleh mereka di industri jaringan atau mereka yang ingin membangun koneksi melalui jaringan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.news

Digunakan untuk mendistribusikan informasi berita seperti peristiwa terkini atau informasi yang berkaitan dengan jurnalisme dan komunikasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ninja

Digunakan oleh individu dan bisnis yang ingin mengasosiasikan diri dengan kemampuan seorang ninja.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sekarang

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.onl

Ekstensi .onl adalah singkatan untuk "online," dan juga merupakan singkatan dalam bahasa Spanyol untuk organisasi nirlaba.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.online

Ekstensi .onl adalah singkatan untuk "online," dan juga merupakan singkatan dalam bahasa Spanyol untuk organisasi nirlaba.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.org

Digunakan oleh semua jenis organisasi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.partners

Digunakan oleh firma hukum, investor, dan berbagai perusahaan. Juga digunakan untuk situs web sosial yang membangun hubungan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.parts

Digunakan sebagai ekstensi umum, tetapi ideal untuk produsen, penjual, dan pembeli suku cadang.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.photo

Digunakan oleh fotografer dan siapa pun yang tertarik dengan foto.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.photography

Digunakan oleh fotografer dan siapa pun yang tertarik dengan foto.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.photos

Digunakan oleh fotografer dan siapa pun yang tertarik dengan foto.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pics

Digunakan oleh fotografer dan siapa pun yang tertarik dengan foto.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pictures

Digunakan oleh siapa pun yang tertarik dengan fotografi, seni, dan media.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pink

Digunakan oleh mereka yang suka warna pink atau mereka yang ingin mengasosiasikan warna pink dengan bisnis atau merek mereka.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pizza

Digunakan oleh restoran pizza dan pecinta pizza.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.place

Digunakan sebagai ekstensi umum, tapi ideal untuk sektor perumahan dan perjalanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.plumbing

Digunakan oleh orang-orang dalam industri pipa saluran air.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.plus

Digunakan sebagai ekstensi umum, namun ideal untuk pakaian ukuran besar, perangkat lunak tambahan, atau produk apa pun yang menawarkan fitur atau dimensi "ekstra".

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.poker

Digunakan oleh pemain dan situs web permainan poker.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.porno

Digunakan untuk situs web khusus dewasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tekan

Digunakan untuk situs web khusus dewasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pro

Digunakan oleh profesional berlisensi dan memiliki kredensial serta organisasi profesional.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.productions

Digunakan oleh studio dan rumah produksi yang membuat iklan, iklan radio, dan video musik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.properties

Digunakan untuk informasi tentang semua jenis properti, termasuk real estat atau kekayaan intelektual. Juga digunakan oleh mereka yang memiliki rumah, bangunan, atau tanah yang ingin dijual atau disewakan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.property

Digunakan untuk informasi tentang semua jenis properti, termasuk real estat atau kekayaan intelektual. Juga digunakan oleh mereka yang memiliki rumah, bangunan, atau tanah yang ingin dijual atau disewakan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .property ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pub

Digunakan oleh orang-orang dalam bisnis publikasi, iklan, atau pembuatan bir.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.qpon

Digunakan untuk kupon dan kode promo.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.recipes

Digunakan oleh mereka yang ingin berbagi resep.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.red

Digunakan oleh mereka yang suka warna merah atau mereka yang ingin mengasosiasikan warna merah dengan bisnis atau merek mereka.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.reise

Digunakan untuk situs web yang berhubungan dengan wisata atau perjalanan. "Reise" adalah kata dalam bahasa Jerman yang berarti "bangkit", "muncul", atau "melakukan perjalanan".

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.reisen

Digunakan untuk situs web yang berhubungan dengan wisata atau perjalanan. "Reisen" adalah kata Jerman yang berarti "bepergian."

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.rentals

Digunakan untuk semua jenis penyewaan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.repair

Digunakan oleh layanan perbaikan atau oleh mereka yang ingin mengajarkan orang lain cara memperbaiki semua jenis barang.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.report

Digunakan sebagai ekstensi umum, namun ideal untuk informasi tentang laporan bisnis, publikasi komunitas, laporan buku, atau pelaporan berita.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.republican

Digunakan untuk informasi tentang Partai Republik (AS). Juga digunakan oleh pejabat yang mencalonkan diri sebagai kantor dewan terpilih, dewan terpilih, penggemar politik, konsultan, dan penasihat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.restaurant

Digunakan oleh industri restoran.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.reviews

Digunakan oleh mereka yang ingin memberikan pendapat dan membaca komentar orang lain.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.rip

Digunakan untuk situs web yang didedikasikan untuk kematian dan peringatan. "RIP" adalah singkatan untuk "rest in peace" (beristirahat dalam damai).

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.rocks

Digunakan sebagai ekstensi umum, tapi ideal untuk siapa saja yang menyukai "rock" (batuan/musik): musisi, ahli geologi, pembuat perhiasan, pendaki, dan banyak lagi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.run

Digunakan sebagai ekstensi umum, tapi ideal untuk industri kebugaran dan olahraga.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sale

Digunakan oleh situs web perdagangan elektronik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sarl

Digunakan oleh perseroan terbatas yang biasanya berlokasi di Prancis. "SARL" adalah singkatan dari Société à Responsabilité Limitée.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.school

Digunakan untuk informasi tentang pendidikan, lembaga pendidikan, dan kegiatan yang berhubungan dengan sekolah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.schule

Digunakan untuk informasi tentang pendidikan, lembaga pendidikan, dan kegiatan yang berhubungan dengan sekolah yang berbasis di Jerman. "Schule" adalah kata bahasa Jerman yang berarti "sekolah".

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.services

Digunakan untuk situs web yang berfokus pada segala jenis layanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sex

Digunakan untuk konten khusus dewasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sexy

Digunakan untuk konten seksual. Juga digunakan untuk menggambarkan merek, produk, informasi, serta situs web yang paling populer dan menarik.

[Return to index](#)

Important

Anda tidak dapat lagi menggunakan Route 53 untuk mendaftarkan domain.sexy baru atau mentransfer domain.sexy ke Route 53. Kami akan terus mendukung domain.sexy yang sudah terdaftar dengan Route 53.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda tidak dapat lagi mentransfer domain.sexy ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.shiksha

Digunakan oleh institusi pendidikan. "Shiksha" adalah istilah dalam bahasa India yang berarti sekolah.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.shoes

Digunakan oleh pengecer sepatu, desainer, produsen, atau blogger mode.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.toko

Digunakan untuk bisnis online dan brick-and-mortar ritel, serta penyedia layanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.belanja

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.show

Digunakan sebagai ekstensi umum, tapi ideal untuk industri hiburan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.singles

Digunakan oleh layanan kencan, resort, dan bisnis lain yang melayani mereka yang ingin menjalin hubungan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sit

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ski

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.soccer

Digunakan untuk situs web yang didedikasikan untuk permainan sepak bola.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.social

Digunakan untuk informasi tentang media sosial, forum, dan percakapan online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.solar

Digunakan untuk informasi tentang tata surya atau energi surya.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.solutions

Digunakan oleh konsultan, do-it-yourself layanan, dan penasihat dari semua jenis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.perangkat lunak

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ruang

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tempat

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.toko

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.aliran

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.studio

Digunakan sebagai ekstensi umum, tapi ideal untuk industri real estat, seni, dan hiburan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.style

Digunakan sebagai ekstensi umum, tetapi ideal untuk situs web yang didedikasikan untuk tren terbaru, terutama tren dalam fashion, desain, arsitektur, dan seni.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.sucks

Digunakan sebagai ekstensi umum, namun ideal bagi mereka yang ingin berbagi pengalaman negatif atau memperingatkan orang lain tentang penipuan atau produk yang cacat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.supplies

Digunakan oleh bisnis yang menjual barang secara online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.supply

Digunakan oleh bisnis yang menjual barang secara online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.support

Digunakan oleh bisnis, grup, atau badan amal yang menawarkan beragam jenis dukungan, termasuk dukungan pelanggan, produk, atau sistem atau dukungan emosional, keuangan, atau spiritual.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.surgery

Digunakan untuk informasi tentang operasi, obat-obatan, dan pemeliharaan kesehatan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.systems

Digunakan terutama oleh industri teknologi dan mereka yang menawarkan layanan teknologi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tattoo

Digunakan oleh peminat tato dan industri tato.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Sirilik (terutama Rusia), Prancis, Jerman, Italia, Portugis, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tax

Digunakan untuk informasi tentang pajak, persiapan pajak, dan hukum pajak.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.taxi

Digunakan oleh taksi, supir, dan perusahaan antar jemput.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.team

Digunakan oleh bisnis atau organisasi yang ingin mengidentifikasi diri mereka sebagai sebuah tim.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tech

Digunakan oleh penggemar teknologi dan mereka yang berdedikasi dalam teknologi di perusahaan, layanan, dan produsen.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.technology

Digunakan oleh penggemar teknologi dan mereka yang berdedikasi dalam teknologi di perusahaan, layanan, dan produsen.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tennis

Digunakan untuk informasi yang berkaitan dengan permainan tenis.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.theater

Digunakan untuk situs web yang didedikasikan untuk teater, drama, dan musikal.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tienda

Digunakan oleh bisnis retail yang ingin terhubung dengan konsumen berbahasa Spanyol.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tips

Digunakan oleh mereka yang ingin berbagi pengetahuan dan saran tentang hampir semua topik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tires

Digunakan oleh produsen, distributor, atau pembeli ban.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.today

Digunakan untuk informasi tentang peristiwa terkini, berita, cuaca, hiburan, dan banyak lagi.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tools

Digunakan untuk informasi tentang berbagai jenis alat.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tours

Digunakan sebagai ekstensi umum, tapi ideal untuk perusahaan perjalanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.town

Digunakan untuk mempromosikan lokasi, budaya, dan komunitas di sebuah kota.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.toys

Digunakan oleh industri mainan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.trade

Digunakan sebagai ekstensi umum, tetapi ideal untuk situs web perdagangan atau layanan perdagangan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Denmark, Jerman, Norwegia, dan Swedia.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.training

Digunakan oleh pelatih dan pendidik.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.tv

Digunakan untuk informasi tentang televisi dan media.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Tidak ada.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.university

Digunakan oleh universitas dan organisasi pendidikan lainnya.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.uno

Digunakan untuk informasi tentang komunitas Hispanik, Portugis, dan Italia.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.vacations

Digunakan oleh industri perjalanan dan pariwisata.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.vegas

Digunakan untuk mempromosikan kota Las Vegas dan gaya hidup Las Vegas.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ventures

Digunakan oleh pengusaha, startup, kapitalis ventura, bank investasi, dan pemodal.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.vg

Lihat [.vg \(Kepulauan Virgin Inggris\)](#).

[Return to index](#)

.viajes

Digunakan oleh agen perjalanan, operator tur, blog perjalanan, perusahaan tur, layanan penyewaan, blogger perjalanan, dan pengecer perjalanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.video

Digunakan oleh industri media dan video.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Tionghoa, Prancis, Jerman, Latin, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.villa

Digunakan oleh agen real estat dan pemilik properti yang memiliki vila untuk dijual atau disewakan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.vision

Digunakan sebagai ekstensi umum, namun ideal untuk spesialis penglihatan seperti optometris dan dokter spesialis mata.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.suara

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.voyage

Digunakan oleh agen perjalanan, operator tur, blog perjalanan, perusahaan tur, layanan penyewaan, blogger perjalanan, dan pengecer perjalanan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.watch

Digunakan untuk informasi tentang situs web streaming, web TVs, video, atau jam tangan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.website

Digunakan untuk informasi tentang pengembangan, promosi, perbaikan, dan pengalaman situs web.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Tionghoa Sederhana, Tionghoa Tradisional, Yunani, Ibrani, Jepang, Korea, dan Thailand.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.pernikahan

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Tidak ada.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Mandarin, Prancis, Jerman, dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa

- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.wiki

Digunakan untuk informasi tentang dokumentasi online.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab dan Latin.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.anggur

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi

Didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.kerja

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.works

Digunakan oleh bisnis, organisasi, dan individu untuk informasi tentang pekerjaan dan layanan ketenagakerjaan. Ekstensi ini dapat digunakan sebagai alternatif ekstensi .com, .net, atau .org.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.world

Digunakan oleh siapa saja yang ingin memberikan informasi tentang subjek global.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.wtf

Digunakan oleh siapa saja yang ingin mengidentifikasi diri dengan akronim populer (tapi tidak senonoh) "WTF".

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.XXX

Digunakan untuk situs web yang meng-host konten khusus dewasa.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.xyz

Digunakan sebagai ekstensi umum untuk tujuan apa pun.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Registri untuk domain .xyz, Generation XYZ, menganggap beberapa nama domain sebagai nama domain premium. Anda tidak dapat mendaftarkan domain .xyz premium atau mentransfernya ke Route 53. Untuk informasi lebih lanjut, lihat situs web [Generation XYZ](#).

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.zone

Digunakan untuk informasi tentang berbagai jenis zona, termasuk zona waktu, zona iklim, dan zona olahraga.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Prancis dan Spanyol.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa

- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

Domain tingkat atas geografis

Ekstensi domain berikut dikelompokkan berdasarkan geografi dan menyertakan ekstensi khusus negara resmi, yang dikenal sebagai domain tingkat atas kode negara (cc). TLDs Contohnya termasuk .be (Belgia), .in (India), dan .mx (Meksiko). Aturan untuk pendaftaran cc TLDs bervariasi menurut negara. Beberapa negara tidak dibatasi, yang berarti bahwa siapa pun di dunia dapat mendaftar, sementara negara lain memiliki batasan tertentu, seperti residensi. Daftar untuk setiap ccTLD menunjukkan adanya pembatasan.

Important

Selama transfer cc apa pun TLDs ke Route 53, kecuali untuk .cc dan .tv, pembaruan ke kontak pemilik diabaikan dan data kontak pemilik dari registri digunakan. Anda dapat memperbarui kontak pemilik setelah transfer selesai. Untuk informasi selengkapnya, lihat [Memperbarui informasi kontak dan kepemilikan domain](#).

[Return to index](#)

Afrika

[.ac \(Pulau Ascension\)](#), [.co.za \(Afrika Selatan\)](#), [.sh \(Saint Helena\)](#)

Amerika

[.ai \(Anguila\)](#), [.ca \(Kanada\)](#), [.cl \(Chili\)](#), [.co \(Kolombia\)](#), [.com.ar \(Argentina\)](#), [.com.br \(Brasil\)](#), [.com.mx \(Meksiko\)](#), [.mx \(Meksiko\)](#), [.us \(Amerika Serikat\)](#), [.vc \(Saint Vincent dan Grenadines\)](#), [.vg \(Kepulauan Virgin Inggris\)](#)

Asia/Oseania

[.au \(Australia\)](#), [.cc \(Pulau Cocos \(Keeling\)\)](#), [.co.nz \(Selandia Baru\)](#), [.com.au \(Australia\)](#), [.com.sg \(Republik Singapura\)](#), [.fm \(Negara Federasi Mikronesia\)](#), [.in \(India\)](#), [.jp \(Jepang\)](#), [.io \(Wilayah](#)

[Samudra Hindia Britania](#)), [.net.au \(Australia\)](#), [.net.nz \(Selandia Baru\)](#), [.nz \(Selandia Baru\)](#), [.org.nz \(Selandia Baru\)](#), [.pw \(Palau\)](#), [.qa \(Qatar\)](#), [.ru \(Federasi Rusia\)](#), [.sg \(Republik Singapura\)](#)

Eropa

[.be \(Belgia\)](#), [.berlin \(kota Berlin di Jerman\)](#), [.ch \(Swiss\)](#), [.co.uk \(Inggris Raya\)](#), [.cz \(Republik Ceko\)](#), [.de \(Jerman\)](#), [.es \(Spanyol\)](#), [.eu \(Uni Eropa\)](#), [.fi \(Finlandia\)](#), [.fr \(Prancis\)](#), [.gg \(Guernsey\)](#), [.im \(Pulau Man\)](#), [.it \(Italia\)](#), [.me \(Montenegro\)](#), [.me.uk \(Inggris Raya\)](#), [.nl \(Belanda\)](#), [.org.uk \(Inggris Raya\)](#), [.ruhr \(wilayah Ruhr, bagian barat Jerman\)](#), [.se \(Swedia\)](#), [.uk \(Inggris Raya\)](#), [.wien \(kota Wina di Austria\)](#)

Afrika

Anda dapat menggunakan domain tingkat atas berikut (TLDs) untuk Afrika untuk mendaftarkan domain dengan Amazon Route 53.

, ,

[Return to index](#)

.ac (Pulau Ascension)

[Return to index](#)

Juga digunakan sebagai TLD generik yang populer bagi mereka di bidang akademi.

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Ditentukan oleh registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 80 hari setelah kedaluwarsa

.co.za (Afrika Selatan)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Hanya domain tingkat dua yang tersedia untuk ekstensi .za. Route 53 mendukung domain tingkat dua .co.za.

Terbuka untuk umum, dengan beberapa pembatasan:

- Pendaftaran terbuka untuk badan hukum yang dapat diidentifikasi (individu dan badan hukum).
- Nama domain harus lolos dari pemeriksaan zona selama proses pendaftaran.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Tidak

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Perpanjangan dapat dilakukan: Hingga satu hari sebelum tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: 1 hari sebelum kedaluwarsa
- Pemulihan dengan registri dapat dilakukan: Antara 1 hari hingga 9 hari setelah kedaluwarsa
- Domain dihapus dari registri: 9 hari setelah kedaluwarsa

.sh (Saint Helena)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 80 hari setelah kedaluwarsa

Amerika

Anda dapat menggunakan domain tingkat atas berikut (TLDs) untuk Amerika untuk mendaftarkan domain dengan Amazon Route 53.

, , , , , , , , , ,

[Return to index](#)

.ai (Anguila)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Pendaftaran: Dua hingga sepuluh tahun. Pembaruan: Dua hingga sembilan tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Perpanjangan terlambat dengan Route 53 dimungkinkan: Hingga 45 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.ca (Kanada)

[Return to index](#)

Varian, dengan (a) atau tanpa (a) tanda aksen, dari nama domain secara otomatis dicadangkan untuk pendaftar dan menjadi bagian dari bundel administratif. Untuk mengaktifkan domain dalam satu bundel, pendaftar harus membuat permintaan pendaftaran untuk domain tersebut. Semua domain dalam bundel harus didaftarkan oleh pendaftar yang sama dan dengan registrar yang sama. Pendaftar juga harus mengajukan permintaan transfer untuk semua domain dalam satu bundel untuk menyelesaikan transfer.

Email konfirmasi dari registri TLD

Saat mendaftarkan domain .ca, Anda akan menerima email berisi tautan ke prosedur penerimaan perjanjian pendaftar. Anda harus menyelesaikan prosedur dalam waktu tujuh hari atau domain Anda tidak akan didaftarkan.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Pendaftaran terbuka untuk individu atau organisasi yang terhubung ke Kanada, seperti yang dijelaskan oleh Persyaratan Kehadiran Kanada untuk Pendaftar.
- Kontak pendaftar: Anda harus memberikan nama hukum lengkap dan tepat dari pemilik domain tersebut.
- Kontak admin dan teknis: Anda harus menentukan Orang sebagai jenis kontak dan memberikan informasi kontak untuk individu yang tinggal di Kanada.
- Anda harus memilih salah satu dari jenis hukum berikut selama proses pendaftaran:
 - ABO: Masyarakat Aborigin (individu atau kelompok) asli Kanada
 - ASS: Asosiasi tidak berbadan hukum di Kanada
 - CCO: Perusahaan di Kanada, atau provinsi atau wilayah Kanada
 - CCT: Warga negara Kanada
 - EDU: Lembaga pendidikan Kanada
 - GOV: Pemerintah atau lembaga pemerintah di Kanada
 - HOP: Rumah sakit di Kanada
 - INB: Suku Indian yang diakui oleh Undang-Undang Indian Kanada
 - LAM: Perpustakaan, arsip, atau museum di Kanada
 - LGR: Perwakilan Hukum Warga Negara atau Penduduk Tetap Kanada
 - MAJ: Her/His Yang Mulia Ratu/Raja
 - OMK: Merek resmi yang terdaftar di Kanada
 - PLT: Partai politik Kanada
 - PRT: Kemitraan yang terdaftar di Kanada
 - RES: Penduduk tetap Kanada
 - TDM: Merek dagang terdaftar di Kanada (oleh jenis pemilik non-Kanada)
 - TRD: Serikat buruh Kanada
 - TRS: Perwalian yang dilakukan di Kanada

Perlindungan privasi

- Orang — Untuk semua kontak, nama kontak, alamat, nomor telepon, nomor faks, dan alamat email disembunyikan, karena [CIRA](#) secara otomatis menerapkan perlindungan privasinya kepada seseorang. Opsi perlindungan privasi hanya akan diterapkan di registrar Whois.

- Perusahaan, asosiasi, atau badan publik - Tidak didukung di tingkat registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: Beragam. Hubungi [AWS Support](#).

Penghapusan pendaftaran domain

Registri untuk domain .ca tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

.cl (Chili)

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .cl baru atau mentransfer domain .cl ke Route 53. Kami akan terus mendukung domain .cl yang sudah terdaftar dengan Route 53.

[Return to index](#)

Periode perpanjangan

Dua tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCodeAPI](#). (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .cl ke Route 53.

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hubungi [AWS Support](#).
- Kemungkinan perpanjangan terlambat dengan Route 53: Hubungi [AWS Support](#).
- Domain dihapus dari Route 53: Hubungi [AWS Support](#).
- Kemungkinan pemulihan dengan registri: Hubungi [AWS Support](#).
- Domain dihapus dari registri: Hubungi [AWS Support](#).

.co (Kolombia)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga lima tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi (berlaku untuk: orang)

Semua informasi disembunyikan.

Jika jenis kontak bukan orang, nama perusahaan dan negara ditampilkan oleh WHOIS.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 45 hari setelah kedaluwarsa
- Domain dihapus dari registri: 50 hari setelah kedaluwarsa

.com.ar (Argentina)

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .com.ar baru atau mentransfer domain .com.ar ke Route 53. Kami akan terus mendukung domain .com.ar yang sudah terdaftar dengan Route 53.

[Return to index](#)

Periode perpanjangan

Satu tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Untuk mencegah transfer yang tidak sah, batasi akses ke alamat email pendaftar dan ke Route 53 APIs yang memungkinkan perubahan kepemilikan, misalnya,.

[UpdateDomainContact](#) Untuk informasi selengkapnya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Domain Route 53](#) di Referensi Otorisasi Layanan dan. [Contoh izin untuk pemilik catatan domain](#)

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .com.ar ke Route 53.

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hubungi [AWS Support](#).
- Kemungkinan perpanjangan terlambat dengan Route 53: Hubungi [AWS Support](#).
- Domain dihapus dari Route 53: Hubungi [AWS Support](#).
- Kemungkinan pemulihan dengan registri: Hubungi [AWS Support](#).
- Domain dihapus dari registri: Hubungi [AWS Support](#).

.com.br (Brasil)

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .com.br baru atau mentransfer domain .com.br ke Route 53. Kami akan terus mendukung domain .com.br yang sudah terdaftar dengan Route 53.

[Return to index](#)

Periode perpanjangan

Satu tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .com.br ke Route 53.

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 30 hari sebelum kedaluwarsa dan tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 119 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 119 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 119 hari setelah kedaluwarsa

.com.mx (Meksiko)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Ditentukan oleh registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.mx (Meksiko)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Ditentukan oleh registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.us (Amerika Serikat)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Registri untuk domain .us tidak mengizinkan nama domain yang berisi salah satu dari tujuh kata yang diidentifikasi dalam "Appendix to Opinion of the Court" [Federal Communications Commission v. Pacifica Foundation No. 77-528](#).

Terbuka untuk umum, dengan satu pembatasan:

- Ekstensi .us ditujukan untuk situs web atau aktivitas yang berlokasi di Amerika Serikat.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 60 hari setelah kedaluwarsa
- Domain dihapus dari registri: 65 hari setelah kedaluwarsa

.vc (Saint Vincent dan Grenadines)

Juga digunakan sebagai TLD generik, sering digunakan oleh mereka yang terlibat dalam pembiayaan modal ventura, perguruan tinggi universitas, dan sebagainya.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 80 hari setelah kedaluwarsa

.vg (Kepulauan Virgin Inggris)

Juga digunakan sebagai TLD generik, sering kali oleh organisasi yang terlibat dalam video game.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga 44 hari setelah tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Ya
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Domain dihapus dari registri: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 74 hari setelah kedaluwarsa
- Domain dibuat tersedia untuk umum lagi: 80 hari setelah kedaluwarsa

Asia/Oseania

Anda dapat menggunakan domain tingkat atas berikut (TLDs) untuk Asia dan Oseania untuk mendaftarkan domain dengan Amazon Route 53.

, , , , , , , , , , , , , , , ,

[Return to index](#)

.au (Australia)

[Return to index](#)

Email konfirmasi dari registri TLD

Rekanan registrar kami, Gandi, menjual kembali domain.au melalui. DomainDirectors Ketika Anda mentransfer nama domain ke Route 53, DomainDirectors mengirimkan email ke kontak pendaftar untuk domain untuk memverifikasi informasi kontak atau untuk mengotorisasi permintaan transfer.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga lima tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Domain.au terbuka untuk badan hukum, perdagangan, kemitraan, atau pedagang tunggal yang terdaftar di Australia; untuk perusahaan asing yang memiliki lisensi untuk berdagang di Australia; dan untuk pemilik atau pelamar merek dagang terdaftar di Australia. Individu tidak dapat mendaftarkan domain.au. Kontak pendaftar harus berupa perusahaan.
- Selama proses pendaftaran, Anda harus menunjukkan hal berikut:
 - Jenis pendaftaran Anda: ABN (Australian Business Number), ACN (Australian Company Number), atau TM (Trademark) jika nama domain sesuai dengan merek dagang Anda.
 - Nomor ID Anda, yang dapat berupa Nama Bisnis Australia (ABN), Nomor Perusahaan Australia (ACN), atau TM (merek dagang).
 - Nama pendaftar Anda, yang merupakan nama badan hukum yang mendaftarkan domain. Nilai ini harus sama persis dengan nama pada ABN (Nomor Bisnis Australia), ACN (Nomor Perusahaan Australia), atau TM (Merek Dagang) yang disediakan.
 - Jenis kelayakan Anda, yang mengacu pada jenis badan hukum yang mendaftarkan nama domain.
 - Alasan mengapa Anda diizinkan untuk mendaftarkan nama domain ini (Alasan kebijakan):
 - Nama domain cocok dengan akronim atau singkatan dari perusahaan pendaftar atau nama dagang, nama organisasi atau asosiasi, atau merek dagang. (Alasan kebijakan 1)
 - Nama domain memenuhi aturan alokasi tetapi bukan akronim atau singkatan dari perusahaan registrant atau nama dagang, nama organisasi atau asosiasi, atau merek dagang. (Alasan kebijakan 2). Untuk melihat aturan alokasi untuk .au, lihat JADWAL A dari registri [.au](#).
- Informasi kontak yang salah atau tidak cocok, termasuk nama, ABN, atau nomor Merek Dagang (TM) akan mengakibatkan kegagalan pendaftaran, perdagangan, dan perpanjangan. Perubahan kepemilikan mungkin diperlukan untuk memperbaiki informasi pada domain yang ada.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya. Selain konsol Route 53, Anda juga dapat memperoleh kode transfer dari [registri .au](#).

DNSSEC

Didukung untuk pendaftaran domain. Ketika Anda mengatur kunci, Anda harus memilih algoritma keamanan DNS 2 (DH). Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 60 hari sebelum kedaluwarsa dan tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 29 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 30 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain.au tidak memungkinkan Anda untuk menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

Mengubah kepemilikan

Ubah pemilik dengan menggunakan konsol Route 53. Lihat [Memperbarui informasi kontak untuk domain](#). Kemudian selesaikan proses berikut untuk menyelesaikan perubahan kepemilikan:

1. Baik pendaftar lama dan baru harus mengklik tautan yang mereka terima dalam email dari transfers@1api.net ke alamat email mereka yang terdaftar. Jika ini tidak selesai dalam 14 hari, Anda harus memulai proses lagi.
2. Setelah tanggapan dikonfirmasi, perubahan pemilik dalam registri akan diproses dalam waktu singkat tanpa konfirmasi lebih lanjut.

.cc (Pulau Cocos (Keeling))

[Return to index](#)

Juga digunakan sebagai TLD generik, sering kali oleh organisasi dengan "cc" dalam nama mereka, seperti perusahaan konsultan, perusahaan komputasi cloud, atau klub bersepeda. Ekstensi ini merupakan alternatif populer dari ".com".

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

- Disembunyikan – alamat, nomor telepon, nomor faks, dan alamat email
- Tidak disembunyikan – nama kontak dan nama organisasi

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 60 hari setelah kedaluwarsa
- Domain dihapus dari registri: 65 hari setelah kedaluwarsa

.co.nz (Selandia Baru)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu harus berusia setidaknya 18 tahun.
- Organisasi harus sudah terdaftar.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 44 hari setelah kedaluwarsa
- Pemulihan dengan registri dimungkinkan: Antara 44 hari dan 134 hari setelah kedaluwarsa
- Domain dihapus dari registri: 134 hari setelah kedaluwarsa

.com.au (Australia)

[Return to index](#)

Email konfirmasi dari registri TLD

Rekanan registrar kami, Gandi, menjual kembali domain.com.au melalui. DomainDirectors Ketika Anda mentransfer nama domain ke Route 53, DomainDirectors mengirimkan email ke kontak pendaftar untuk domain untuk memverifikasi informasi kontak atau untuk mengotorisasi permintaan transfer.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga lima tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Domain .com.au dan .net.au terbuka untuk kemitraan atau pedagang tunggal yang terdaftar di Australia; untuk perusahaan asing yang memiliki lisensi untuk berdagang di Australia; dan untuk pemilik atau pelamar merek dagang terdaftar di Australia. Individu tidak dapat mendaftarkan domain .com.au/.net.au. Kontak pendaftar harus berupa perusahaan.
- Nama domain Anda harus identik dengan nama Anda (sebagaimana terdaftar pada otoritas Australia yang relevan) atau dengan merek dagang Anda (atau singkatan atau akronim merek dagang Anda).
- Nama domain harus menunjukkan aktivitas Anda. Misalnya, nama domain harus menunjukkan produk yang Anda jual atau layanan yang Anda berikan.
- Selama proses pendaftaran, Anda harus memberikan informasi berikut:
 - Jenis pendaftaran Anda: ABN (Australian Business Number), ACN (Australian Company Number), atau TM (Trademark) jika nama domain sesuai dengan merek dagang Anda.
 - Nomor ID Anda, yang dapat berupa Nomor Bisnis Australia (ABN), Nomor Perusahaan Australia (ACN), atau nomor merek dagang Anda (TM) jika nama domain sesuai dengan merek dagang Anda.
 - Nama pendaftar Anda, yang merupakan nama badan hukum yang mendaftarkan domain. Nilai ini harus sama persis dengan nama yang disediakan.
 - Jenis kelayakan Anda, yang mengacu pada jenis badan hukum yang mendaftarkan nama domain ini.
 - Alasan mengapa Anda diizinkan untuk mendaftarkan nama domain ini (Alasan kebijakan):

- Nama domain cocok dengan akronim atau singkatan dari perusahaan pendaftar atau nama dagang, nama organisasi atau asosiasi, atau merek dagang. (Alasan kebijakan 1)
- Nama domain memenuhi aturan alokasi tetapi bukan akronim atau singkatan dari perusahaan pendaftar atau nama dagang, nama organisasi atau asosiasi, atau merek dagang. (Alasan kebijakan 2). Untuk melihat aturan alokasi untuk .com.au, lihat JADWAL C dari registri [.com.au](https://www.austlii.edu.au/au/other/dfat/special/com.au/).
- Informasi kontak yang salah atau tidak cocok, termasuk nama, ABN, atau nomor Merek Dagang (TM) akan mengakibatkan kegagalan pendaftaran, perdagangan, dan perpanjangan. Perubahan kepemilikan mungkin diperlukan untuk memperbaiki informasi pada domain yang ada.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Ketika Anda mengatur kunci, Anda harus memilih algoritma keamanan DNS 2 (DH). Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 60 hari sebelum kedaluwarsa dan tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 29 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 30 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .com.au tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

Mengubah kepemilikan

Ubah pemilik, baik secara terprogram atau dengan menggunakan konsol Route 53. Lihat [Memperbarui informasi kontak untuk domain](#). Kemudian selesaikan proses berikut untuk menyelesaikan perubahan kepemilikan:

1. Baik pendaftar lama dan baru harus mengklik tautan yang mereka terima dalam email dari transfers@1api.net ke alamat email mereka yang terdaftar. Jika ini tidak selesai dalam 14 hari, Anda harus memulai proses lagi.
2. Setelah tanggapan dikonfirmasi, perubahan pemilik dalam registri akan diproses dalam waktu singkat tanpa konfirmasi lebih lanjut.

.com.sg (Republik Singapura)

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .com.sg baru atau mentransfer domain .com.sg ke Route 53. Kami akan terus mendukung domain .com.sg yang sudah terdaftar dengan Route 53.

[Return to index](#)

Periode perpanjangan

Satu atau dua tahun.

Penghapusan pendaftaran domain

Registri untuk domain .com.sg tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .com.sg ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 60 hari setelah kedaluwarsa
- Domain dihapus dari registri: 60 hari setelah kedaluwarsa

.fm (Negara Federasi Mikronesia)

Juga digunakan sebagai TLD generik, sering kali oleh organisasi yang terlibat dalam media online dan penyiaran.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 44 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 44 hari hingga 79 hari setelah kedaluwarsa
- Domain dihapus dari registri: 84 hari setelah kedaluwarsa

.in (India)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 60 hari setelah kedaluwarsa
- Domain dihapus dari registri: 65 hari setelah kedaluwarsa

.jp (Jepang)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, dengan satu pembatasan:

- Hanya individu atau perusahaan yang berlokasi di Jepang yang dapat mendaftarkan nama domain .jp.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route

53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Jepang.

Kode otorisasi diperlukan untuk transfer

Ya.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Perpanjangan dimungkinkan: Hingga 16 hari sebelum tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: 6 hari sebelum kedaluwarsa
- Kemungkinan pemulihan dengan registri: Hubungi [AWS Support](#).
- Domain dihapus dari registri: Hubungi [AWS Support](#).

 Note

Mendaftarkan domain non-general-purpose JP seperti .co.jp dan .or.jp saat ini tidak memungkinkan.

.io (Wilayah Samudra Hindia Britania)

Juga digunakan sebagai TLD generik, sering kali oleh organisasi yang berhubungan dengan komputer seperti layanan online, game berbasis peramban, dan perusahaan rintisan.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Semua informasi disembunyikan kecuali state/province dan negara.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

Registri untuk domain .io juga menggunakan kode otorisasi sebagai kata sandi sekali pakai untuk beberapa operasi, seperti mengaktifkan atau menonaktifkan perlindungan privasi. Jika ingin melakukan lebih dari satu operasi yang memerlukan kata sandi, Anda harus menghasilkan kode otorisasi lain untuk setiap operasi.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 90 hari setelah kedaluwarsa

.net.au (Australia)

[Return to index](#)

Email konfirmasi dari registri TLD

Rekanan registrar kami, Gandi, menjual kembali domain.net.au melalui. DomainDirectors

Ketika Anda mentransfer nama domain ke Route 53, DomainDirectors mengirimkan email ke

kontak pendaftar untuk domain untuk memverifikasi informasi kontak atau untuk mengotorisasi permintaan transfer.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga lima tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Domain .com.au dan .net.au terbuka untuk badan hukum, perdagangan, kemitraan, atau pedagang tunggal yang terdaftar di Australia; untuk perusahaan asing yang memiliki lisensi untuk berdagang di Australia; dan untuk pemilik atau pelamar merek dagang terdaftar di Australia.
- Nama domain Anda harus identik dengan nama Anda, sebagaimana terdaftar pada otoritas Australia yang relevan, atau dengan merek dagang Anda (atau singkatan atau akronim merek dagang Anda).
- Nama domain harus menunjukkan aktivitas Anda. Misalnya, nama domain harus menunjukkan produk yang Anda jual atau layanan yang Anda berikan.
- Selama proses pendaftaran, Anda harus menunjukkan hal berikut:
 - Jenis pendaftaran Anda: ABN (Australian Business Number), ACN (Australian Company Number), atau TM (Trademark) jika nama domain sesuai dengan merek dagang Anda.
 - Nomor ID Anda, yang dapat berupa Nomor Bisnis Australia (ABN), Nomor Perusahaan Australia (ACN), atau nomor merek dagang Anda (TM) jika nama domain sesuai dengan merek dagang Anda.
 - Nama pendaftar Anda, yang merupakan nama badan hukum yang mendaftarkan domain. Nilai ini harus sama persis dengan nama yang disediakan.
 - Jenis kelayakan Anda, yang mengacu pada jenis badan hukum yang mendaftarkan nama domain ini.
 - Alasan mengapa Anda diizinkan untuk mendaftarkan nama domain ini (Alasan kebijakan):
 - Nama domain cocok dengan akronim atau singkatan dari perusahaan pendaftar atau nama dagang, nama organisasi atau asosiasi, atau merek dagang. (Alasan kebijakan 1)
 - Nama domain memenuhi aturan alokasi tetapi bukan akronim atau singkatan dari perusahaan pendaftar atau nama dagang, nama organisasi atau asosiasi, atau merek dagang. (Alasan kebijakan 2). [Untuk melihat aturan alokasi untuk.net.au, lihat JADWAL E dari registri net.au.](#)

- Informasi kontak yang salah atau tidak cocok, termasuk nama, ABN, atau nomor Merek Dagang (TM) akan mengakibatkan kegagalan pendaftaran, perdagangan, dan perpanjangan. Perubahan kepemilikan mungkin diperlukan untuk memperbaiki informasi pada domain yang ada.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Ketika Anda mengatur kunci, Anda harus memilih algoritma keamanan DNS 2 (DH). Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 60 hari sebelum kedaluwarsa dan tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 29 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 30 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .net.au tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

Mengubah kepemilikan

Ubah pemilik, baik secara terprogram atau dengan menggunakan konsol Route 53. Lihat [Memperbarui informasi kontak untuk domain](#). Kemudian selesaikan proses berikut untuk menyelesaikan perubahan kepemilikan:

1. Baik pendaftar lama dan baru harus mengklik tautan yang mereka terima dalam email dari `transfers@1api.net` ke alamat email mereka yang terdaftar. Jika ini tidak selesai dalam 14 hari, Anda harus memulai proses lagi.
2. Setelah tanggapan dikonfirmasi, perubahan pemilik dalam registri akan diproses dalam waktu singkat tanpa konfirmasi lebih lanjut.

.net.nz (Selandia Baru)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu harus berusia setidaknya 18 tahun.
- Organisasi harus sudah terdaftar.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 44 hari setelah kedaluwarsa
- Pemulihan dengan registri dimungkinkan: Antara 44 hari dan 134 hari setelah kedaluwarsa
- Domain dihapus dari registri: 134 hari setelah kedaluwarsa

.nz (Selandia Baru)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu harus berusia setidaknya 18 tahun.
- Organisasi harus sudah terdaftar.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 44 hari setelah kedaluwarsa
- Pemulihan dengan registri dimungkinkan: Antara 44 hari dan 134 hari setelah kedaluwarsa
- Domain dihapus dari registri: 134 hari setelah kedaluwarsa

.org.nz (Selandia Baru)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu harus berusia setidaknya 18 tahun.
- Organisasi harus sudah terdaftar.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route

53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 44 hari setelah kedaluwarsa
- Pemulihan dengan registri dimungkinkan: Antara 44 hari dan 134 hari setelah kedaluwarsa
- Domain dihapus dari registri: 134 hari setelah kedaluwarsa

.pw (Palau)

[Return to index](#)

.pw awalnya disediakan untuk penduduk Palau, sebuah negara pulau di sub wilayah Mikronesia Oseania di Pasifik barat, namun, sekarang umumnya digunakan untuk mewakili 'Web Profesional' dan tersedia untuk semua orang.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Perlindungan privasi (berlaku untuk semua jenis kontak: orang, perusahaan, asosiasi, dan lembaga publik)

Semua informasi disembunyikan kecuali nama organisasi.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 75 hari setelah kedaluwarsa

.qa (Qatar)

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .qa baru atau mentransfer domain .qa ke Route 53. Kami akan terus mendukung domain .qa yang sudah terdaftar dengan Route 53.

[Return to index](#)

Periode perpanjangan

Satu hingga lima tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53

ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .qa ke Route 53.

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 31 hari setelah kedaluwarsa

.ru (Federasi Rusia)

Important

Anda tidak dapat lagi menggunakan Route 53 untuk mendaftarkan domain .ru baru, mentransfer domain .ru ke Route 53, atau memperbarui domain .ru yang ada dengan Route 53. Jika Anda memiliki domain .ru yang ada dengan Route 53, transfer ke registrar yang mendukung .ru segera untuk menghindari gangguan layanan apa pun.

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Note

Registri untuk domain .ru memperbarui tanggal kedaluwarsa domain pada hari domain kedaluwarsa. Kueri WHOIS akan menampilkan tanggal kedaluwarsa lama untuk domain

tersebut hingga tanggal tersebut, terlepas dari kapan Anda memperpanjang domain dengan Route 53.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu mungkin perlu memberikan nomor paspor atau nomor ID yang diterbitkan pemerintah.
- Perusahaan asing mungkin perlu memberikan ID perusahaan atau pendaftaran perusahaan.

Perlindungan privasi

Ditentukan oleh registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .ru ke Route 53.

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

Tidak didukung. Anda tidak dapat lagi memperbarui atau memulihkan domain .ru dengan Route 53.

Penghapusan pendaftaran domain

Registri untuk domain .ru tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

.sg (Republik Singapura)

Important

Anda sudah tidak dapat menggunakan Route 53 untuk mendaftarkan domain .sg baru atau mentransfer domain .sg ke Route 53. Kami akan terus mendukung domain .sg yang sudah terdaftar dengan Route 53.

[Return to index](#)

Periode perpanjangan

Satu atau dua tahun.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Tidak didukung. Anda sudah tidak dapat mentransfer domain .sg ke Route 53.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 60 hari setelah kedaluwarsa
- Domain dihapus dari registri: 60 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .sg tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

- Domain dihapus dari registri: 40 hari setelah kedaluwarsa

.berlin (kota Berlin di Jerman)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Kontak pemilik, administratif, atau teknis harus memberikan alamat di Berlin, dan kontak administratif harus berupa perorangan.
- Anda harus mengaktifkan dan menggunakan domain .berlin dalam waktu 12 bulan setelah pendaftaran (berlaku untuk situs web, pengalihan, atau alamat email).
- Jika Anda memublikasikan situs web di bawah domain .berlin, atau jika domain .berlin mengalihkan ke situs web lain, konten situs web harus terkait dengan Berlin.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Latin dan Sirilik.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa

- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 80 hari setelah kedaluwarsa

.ch (Swiss)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 9 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 9 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 9 hari hingga 49 hari setelah kedaluwarsa

- Domain dihapus dari registri: 49 hari setelah kedaluwarsa

.co.uk (Inggris Raya)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Jika mentransfer domain .co.uk ke Route 53, Anda tidak perlu mendapatkan kode otorisasi. Sebaliknya, gunakan metode yang disediakan oleh registrar domain Anda saat ini untuk memperbarui nilai tanda IPS untuk domain menjadi GANDI, semua huruf besar. (Tanda IPS diperlukan oleh Nominet, registri untuk nama domain .uk.) Jika registrar Anda tidak mengubah nilai tanda IPS, [hubungi Nominet](#).

 Note

Saat Anda mendaftarkan domain .co.uk, Route 53 secara otomatis menetapkan tanda IPS untuk domain menjadi GANDI.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 180 hari sebelum hingga 30 hari setelah tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Antara 30 hari hingga 90 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 90 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 92 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .co.uk tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

.cz (Republik Ceko)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung, namun alamat email dan nomor telepon untuk semua kontak akan disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

Jika registrar Anda saat ini tidak memberikan kode otorisasi, buka <https://www.nic.cz/whois/send-password/> untuk memintanya dikirim ke alamat email pendaftar oleh registri domain CZ.

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 58 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 59 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 60 hari setelah kedaluwarsa

.de (Jerman)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Anda harus berdomisili di Jerman atau memiliki kontak administratif (manusia) yang berdomisili di Jerman dan memiliki alamat selain kotak P.O.
- Selama pendaftaran, DNS (A, MX, dan CNAME) nama domain harus dikonfigurasi dengan benar sehingga dapat lolos dari pemeriksaan zona registri. Diperlukan tiga server dari dua kelas C yang berbeda.
- Jika Anda menggunakan layanan DNS selain Route 53, server nama untuk domain harus lolos dari pemeriksaan untuk memastikan bahwa mereka dikonfigurasi dengan benar. Untuk menentukan apakah server nama untuk domain Anda akan lulus cek, lihat <https://www.denic.de/en/service/tools/nast/>.
- Anda harus memberikan informasi kontak yang memenuhi persyaratan validasi registri. Detail kontak yang tidak valid atau salah format dapat menyebabkan perpanjangan domain gagal.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: Pada tanggal kedaluwarsa
- Kemungkinan pemulihan dengan registri: Hubungi [AWS Support](#).
- Domain dihapus dari registri: Hubungi [AWS Support](#).

.es (Spanyol)

[Return to index](#)

Pembelian atau transfer domain

Important

Saat ini Anda dapat membeli nama domain.es baru atau mentransfer domain.es ke Route 53. Jenis kontak untuk kontak pendaftar tidak memiliki batasan. Admin/Teknik/Jenis kontak penagihan harus berupa seseorang.

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga lima tahun.

Pembatasan

Terbuka untuk umum, bagi mereka yang memiliki minat dalam atau berhubungan dengan Spanyol.

Mulai 2016, pendaftar domain.ES harus memberikan email kontak pendaftar. Jika Anda belum memberikan informasi ini, Anda harus melakukannya di registrar saat ini sebelum mentransfer domain Anda ke Route 53.

Anda akan memerlukan informasi berikut:

- Pengidentifikasi ESNIC mirip dengan. **AAAA0-ESNIC-F0**
- Jika Anda tidak tahu pengenalan ESNIC Anda, Anda bisa mendapatkannya dari registrar saat ini. Anda dapat menemukan registrar Anda di: <https://www.dominios.es/en>.

Bergantung pada apakah Anda mengingat kata sandi di registrar, atau tidak, Anda dapat mengikuti salah satu prosedur berikut untuk memperbarui email pendaftar Anda:

- Jika Anda ingat kata sandi Anda, masuk di <https://www.nic.es/sgnd/login.action> dengan menggunakan identifikasi dan kata sandi ESNIC Anda.

Setelah masuk, Anda dapat mengedit kontak email pendaftar dengan memilih tab Edit pada halaman registri.

- Jika Anda lupa kata sandi, telusuri https://www.nic.es/sgnd/peticion/editCorreo.tindakan?request_locale=id.

Isi formulir dengan pengenalan ESNIC Anda, kontak email pendaftar Anda yang baru dan valid. Kemudian, validasi formulir dengan memilih Processing tanpa EID/Certificate, dan upload dokumen identitas yang diminta.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

Registri .es mengelola kode otorisasi dengan a time-to-live dan mungkin kedaluwarsa. Anda dapat menyegarkan kode autentikasi dengan menghapus status transfer lock (clientTransferProhibited) dari domain Anda jika ada. Jika domain tidak memiliki kunci transfer, Anda dapat menyegarkan kode autentikasi dengan menyalakannya terlebih dahulu, lalu mematikannya.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Perpanjangan dapat dilakukan: Hingga 6 hari sebelum tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: 6 hari sebelum kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 6 hari sebelum hingga 4 hari setelah kedaluwarsa
- Domain dihapus dari registri: 4 hari setelah kedaluwarsa

.eu (Uni Eropa)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan satu pembatasan:

- Anda harus memberikan alamat pos yang valid di salah satu dari 30 negara bagian Wilayah Ekonomi Eropa (EEA) atau jika Anda adalah warga negara di salah satu dari 27 negara anggota Uni Eropa (EU), Anda harus menentukan negara kewarganegaraan Uni Eropa Anda.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

[Anda juga dapat membuat kode autentikasi dengan menggunakan panel “My.eu” di registri: <https://my.eurid.eu/>.](#)

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: Pada tanggal kedaluwarsa
- Kemungkinan pemulihan dengan registri: Hingga 40 hari setelah kedaluwarsa
- Domain dihapus dari registri: 40 hari setelah kedaluwarsa

Pencarian WHOIS

Untuk informasi tentang domain .eu yang ada, lihat <https://whois.eurid.eu/en/>.

.fi (Finlandia)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga lima tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Perpanjangan .fi tersedia untuk individu yang berdomisili di Finlandia dan memiliki nomor identitas Finlandia, serta badan hukum atau pengusaha swasta yang terdaftar di Finlandia.
- Jika alamat kontak pendaftar berada di Finlandia, maka nomor identitas Finlandia diperlukan untuk pendaftar perorangan dan nomor perusahaan Finlandia diperlukan untuk pendaftar perusahaan, dan Anda harus memberikan informasi berikut saat pendaftaran:
 - Apakah kontak didasarkan pada orang fisik atau moral di Finlandia atau tidak.
 - Pengenal pendaftar dengan nama yang dicatat, jika berdasarkan nama orang moral.
 - Nomor catatan dalam pendaftaran tempat nama dicatat, jika berdasarkan nama orang moral.
 - Nomor identifikasi untuk orang moral di Finlandia.
 - Nomor identifikasi untuk orang fisik di Finlandia.
 - Jika pendaftar adalah Perusahaan Non-Finlandia, maka Anda harus memberikan Nomor Bisnis sebagai VAT_Number.
- Jika alamat pendaftar tidak berlokasi di Finlandia, maka tidak diperlukan identitas atau nomor perusahaan Finlandia.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route

53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: Tidak

Penghapusan pendaftaran domain

Untuk informasi tentang menghapus domain, lihat [Menghapus pendaftaran nama domain](#).

.fr (Prancis)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu harus berusia minimal 18 tahun dan harus menyediakannyadate-of-birth.
- Organisasi harus berlokasi di Wilayah Ekonomi Eropa atau di Swiss.
- Organisasi harus mengisi semua bidang identifikasi perusahaan (nomor PPN, SIREN, WALDEC, DUNS, dan sebagainya), karena ini akan memfasilitasi verifikasi yang mungkin dilakukan AFNIC di kemudian hari.

- Kondisi kelayakan yang sama berlaku untuk kontak administratif.
- Nama dan ketentuan tunduk pada tinjauan AFNIC sebelumnya (Naming Charter Article 2.4) dan ketentuan tambahan berikut:
 - Nama domain yang sebelumnya dipesan atau dilarang terbuka bagi pelamar dengan hak yang sah dan bertindak dengan itikad baik.
 - Nama yang diawali dengan ville, mairie, agglo, cc, cg, dan cr tunduk pada konvensi penamaan AFNIC.

Perlindungan privasi

Ditentukan oleh registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 27 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 28 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 28 hari hingga 58 hari setelah kedaluwarsa
- Domain dihapus dari registri: 58 hari setelah kedaluwarsa

.gg (Guernsey)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 35 hari setelah kedaluwarsa
- Domain dihapus dari registri: 35 hari setelah kedaluwarsa

.im (Pulau Man)

Juga digunakan sebagai TLD generik, sering kali oleh layanan olahpesan instan atau untuk individu yang ingin mengembangkan merek pribadi "Saya".

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu atau dua tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 30 hari setelah kedaluwarsa

.it (Italia)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Individu atau organisasi harus memiliki alamat yang terdaftar di Uni Eropa.
- Jika negara asal Anda adalah Italia, Anda harus memasukkan kode fiskal. Jika negara asal Anda berada di Uni Eropa, Anda harus memasukkan nomor dokumen identitas (nomor ID).
- Server nama untuk domain Anda harus lolos dari pemeriksaan DNS. Kami menyarankan agar Anda memeriksa server nama di <https://dns-check.nic.it/> sebelum mengirimkan permintaan

perubahan. Jika nama domain Anda tidak memenuhi persyaratan teknis (misalnya, nama domain tidak terkait dengan server nama operasional), dan Anda tidak memperbaikinya dalam waktu 30 hari, nama domain Anda akan dihapus oleh registri. Kami tidak mengeluarkan pengembalian dana untuk domain yang dihapus karena tidak memenuhi persyaratan teknis.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#) API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Tidak didukung.

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 13 hari setelah kedaluwarsa
- Domain dihapus dari registri: 49 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 14 hari hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari registri: Hubungi [AWS Support](#).

.me (Montenegro)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Domain .me, registri untuk domain .me, menganggap nama domain dua huruf dan beberapa nama domain yang lebih panjang sebagai nama domain premium. Anda tidak dapat mendaftarkan domain .me premium atau mentransfernya ke Route 53. Untuk informasi lebih lanjut tentang nama domain .me premium, lihat situs web domain.me.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Arab, Belarusia, Bosnia, Bulgaria, Tionghoa Sederhana, Tionghoa Tradisional, Kroasia, Denmark, Prancis, Jerman, Hindi, Hungaria, Islandia, Italia, Korea, Latvia, Lituania, Mongolia, Montenegro, Polandia, Portugis, Rusia, Serbia, Spanyol, Swedia, Turki, dan Ukraina.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 29 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 30 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 30 hari hingga 60 hari setelah kedaluwarsa
- Domain dihapus dari registri: 65 hari setelah kedaluwarsa

.me.uk (Inggris Raya)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Jika mentransfer domain .me.uk ke Route 53, Anda tidak perlu mendapatkan kode otorisasi. Sebaliknya, gunakan metode yang disediakan oleh registrar domain Anda saat ini untuk memperbarui nilai tanda IPS untuk domain menjadi GANDI, semua huruf besar. (Tanda IPS diperlukan oleh Nominet, registri untuk nama domain .uk.) Jika registrar Anda tidak mengubah nilai tanda IPS, [hubungi Nominet](#).

Note

Saat Anda mendaftarkan domain .me.uk, Route 53 secara otomatis menetapkan tanda IPS untuk domain menjadi GANDI.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 180 hari sebelum hingga 30 hari setelah tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Antara 30 hari hingga 90 hari setelah kedaluwarsa

- Domain dihapus dari Route 53: 90 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 92 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .me.uk tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

.nl (Belanda)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Pemilik atau kontak administratif harus memberikan alamat yang valid di Belanda. Kehadiran lokal diperlukan.
- Jika Anda tidak memiliki alamat yang valid di Belanda, SIDN Registri akan menyediakan Anda dengan alamat domisili, sesuai Prosedur Alamat Domisili.
- Nama domain harus terdiri dari 3-63 karakter, tidak termasuk .nl.

Perlindungan privasi

Ditentukan oleh registri.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCodeAPI](#). (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Perpanjangan dapat dilakukan: Hingga 1 hari sebelum tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: 1 hari sebelum kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 1 hari sebelum hingga 39 hari setelah kedaluwarsa
- Domain dihapus dari registri: 39 hari setelah kedaluwarsa

.org.uk (Inggris Raya)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Jika mentransfer domain .org.uk ke Route 53, Anda tidak perlu mendapatkan kode otorisasi. Sebaliknya, gunakan metode yang disediakan oleh registrar domain Anda saat ini untuk

memperbarui nilai tanda IPS untuk domain menjadi GANDI, semua huruf besar. (Tanda IPS diperlukan oleh Nominet, registri untuk nama domain .uk.) Jika registrar Anda tidak mengubah nilai tanda IPS, [hubungi Nominet](#).

 Note

Saat Anda mendaftarkan domain .org.uk, Route 53 secara otomatis menetapkan tanda IPS untuk domain menjadi GANDI.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 180 hari sebelum hingga 30 hari setelah tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Antara 30 hari hingga 90 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 90 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 92 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .org.uk tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

.ruhr (wilayah Ruhr, bagian barat Jerman)

[Return to index](#)

Ekstensi .ruhr diperuntukkan bagi wilayah Ruhr (bagian barat Jerman).

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan satu pembatasan:

- Kontak administratif harus merupakan individu yang memiliki alamat di Jerman.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung (ä, ö, ü, ß).

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: Hubungi [AWS Support](#).

.se (Swedia)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Jika berdomisili di Swedia, Anda harus memberikan nomor ID Swedia yang valid. Format nomor ID adalahYYMMDD-NNNN.
- Jika berada di luar Swedia, Anda harus memasukkan nomor ID yang valid seperti nomor ID pajak.

Persyaratan verifikasi tambahan

Mulai 1 Oktober 2025, pendaftaran domain.se memerlukan verifikasi identitas tambahan untuk mematuhi persyaratan NIS 2.0 baru registri. Saat Anda mendaftarkan domain.se, kami akan menghubungi Anda untuk meminta dokumen verifikasi. Pendaftaran domain Anda akan tetap tertunda sampai Anda memberikan dokumen yang diperlukan dan verifikasi selesai. Untuk mengirimkan dokumen Anda, [hubungi AWS Support](#).

Registri .se juga melakukan audit berkala terhadap domain yang ada dan mungkin meminta verifikasi tambahan untuk domain yang baru terdaftar atau ketika Anda membuat perubahan tertentu pada domain Anda (seperti memperbarui pemilik domain atau informasi kontak). Jika domain Anda ditempatkan dalam serverHold status, ini berarti registri memerlukan verifikasi sebelum domain Anda dapat diaktifkan sepenuhnya.

Dokumen yang harus Anda berikan:

- Untuk perorangan: Dokumen identitas yang dikeluarkan pemerintah (seperti kartu identitas atau paspor) dan bukti alamat yang berusia kurang dari 3 bulan.
- Untuk perusahaan atau organisasi: Sertifikat pendaftaran perusahaan atau organisasi, dan bukti alamat jika berbeda dari sertifikat pendaftaran.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Tidak didukung. Kami menyarankan Anda mencegah transfer yang tidak sah dengan membatasi akses ke tindakan [RetrieveDomainAuthCode](#)API. (Saat Anda membatasi akses ke API Route 53 ini, Anda juga membatasi siapa yang dapat membuat kode otorisasi menggunakan konsol Route 53 AWS SDKs, dan metode terprogram lainnya.) Untuk informasi selengkapnya, lihat [Identity and access management di Amazon Route 53](#).

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Latin, Swedia, dan Yiddish.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Perpanjangan dapat dilakukan: Hingga 1 hari sebelum tanggal kedaluwarsa
- Keterlambatan perpanjangan Route 53 diperbolehkan: Tidak
- Domain dihapus dari Route 53: 1 hari sebelum kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 1 hari sebelum hingga 59 hari setelah kedaluwarsa
- Domain dihapus dari registri: 64 hari setelah kedaluwarsa

.uk (Inggris Raya)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, tanpa pembatasan.

Perlindungan privasi

Semua informasi disembunyikan.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung

Nama domain yang diinternasionalisasi

Tidak didukung.

Kode otorisasi diperlukan untuk transfer

Jika mentransfer domain .uk ke Route 53, Anda tidak perlu mendapatkan kode otorisasi. Sebaliknya, gunakan metode yang disediakan oleh registrar domain Anda saat ini untuk

memperbarui nilai tanda IPS untuk domain menjadi GANDI, semua huruf besar. (Tanda IPS diperlukan oleh Nominet, registri untuk nama domain .uk.) Jika registrar Anda tidak mengubah nilai tanda IPS, [hubungi Nominet](#).

 Note

Saat Anda mendaftarkan domain .uk, Route 53 secara otomatis menetapkan tanda IPS untuk domain menjadi GANDI.

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Antara 180 hari sebelum hingga 30 hari setelah tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Antara 30 hari hingga 90 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 90 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Tidak
- Domain dihapus dari registri: 92 hari setelah kedaluwarsa

Penghapusan pendaftaran domain

Registri untuk domain .uk tidak mengizinkan Anda menghapus pendaftaran domain. Sebaliknya, Anda harus menonaktifkan perpanjangan otomatis dan menunggu hingga domain kedaluwarsa. Untuk informasi selengkapnya, lihat [Menghapus pendaftaran nama domain](#).

.wien (kota Wina di Austria)

[Return to index](#)

Masa sewa untuk pendaftaran dan perpanjangan

Satu hingga sepuluh tahun.

Pembatasan

Terbuka untuk umum, dengan beberapa pembatasan:

- Anda harus menunjukkan ketertarikan ekonomi, budaya, turis, sejarah, sosial, atau lainnya dengan kota Wina di Austria.
- Nama domain .wien harus digunakan sehubungan dengan ketentuan di atas, selama masa pendaftaran.

Perlindungan privasi

Tidak didukung.

Penguncian domain untuk mencegah transfer yang tidak diotorisasi

Didukung.

Nama domain yang diinternasionalisasi

Didukung untuk bahasa Latin.

Kode otorisasi diperlukan untuk transfer

Ya

DNSSEC

Didukung untuk pendaftaran domain. Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

Tenggat waktu untuk memperbarui dan memulihkan domain

- Kemungkinan perpanjangan: Hingga tanggal kedaluwarsa
- Kemungkinan perpanjangan terlambat dengan Route 53: Hingga 44 hari setelah kedaluwarsa
- Domain dihapus dari Route 53: 45 hari setelah kedaluwarsa
- Kemungkinan pemulihan dengan registri: Antara 45 hari hingga 75 hari setelah kedaluwarsa
- Domain dihapus dari registri: 80 hari setelah kedaluwarsa

Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda

Anda dapat menggunakan Amazon Route 53 sebagai layanan DNS untuk domain, seperti example.com. Saat menjadi layanan DNS, Route 53 merutekan lalu lintas internet ke situs web dengan menerjemahkan nama domain yang ramah seperti www.example.com ke dalam alamat IP numerik, seperti 192.0.2.1 yang digunakan komputer untuk terhubung satu sama lain. Ketika seseorang mengetik nama domain Anda di peramban atau mengirimkan email kepada Anda, kueri DNS diteruskan ke Route 53, yang merespons dengan nilai yang sesuai. Misalnya, Route 53 mungkin merespons dengan alamat IP untuk server web example.com.

Hosting DNS vs. pendaftaran domain

Bab ini mencakup penggunaan Route 53 hanya untuk hosting DNS. Ini berarti pendaftaran domain Anda tetap dengan registrar Anda saat ini, dan Anda akan terus membayar mereka untuk perpanjangan domain. Route 53 hanya akan mengelola pengaturan DNS Anda dan menangani kueri DNS untuk domain Anda.

Jika Anda ingin mentransfer pendaftaran domain Anda ke Route 53 juga (membuat Route 53 baik registrar dan layanan DNS Anda), lihat [Daftar periksa pra-transfer untuk transfer domain](#) dan [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#)

Dalam Bab ini, kami menjelaskan cara mengkonfigurasi Route 53 untuk merutekan lalu lintas internet Anda ke tempat yang tepat. Kami juga menjelaskan cara memigrasi layanan DNS ke Route 53 jika Anda saat ini menggunakan layanan DNS lain, dan cara menggunakan Route 53 sebagai layanan DNS untuk domain baru.

Topik

- [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#)
- [Mengonfigurasi perutean DNS untuk domain baru](#)
- [Merutekan lalu lintas ke sumber daya](#)
- [Bekerja dengan zona yang di-hosting](#)
- [Bekerja dengan catatan](#)
- [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#)
- [Menggunakan AWS Cloud Map untuk membuat catatan dan pemeriksaan kesehatan](#)

- [Kendala dan perilaku DNS](#)
- [Topik terkait](#)

Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada

Jika Anda mentransfer satu atau beberapa pendaftaran domain ke Route 53, dan saat ini menggunakan registrar domain yang tidak menyediakan layanan DNS berbayar, Anda harus memigrasi layanan DNS sebelum memigrasi domain. Jika tidak, registrar akan berhenti menyediakan layanan DNS saat Anda mentransfer domain, dan situs web serta aplikasi web yang terkait akan menjadi tidak tersedia di internet. (Anda juga dapat memigrasi layanan DNS dari registrar saat ini ke penyedia layanan DNS lainnya. Kami tidak mengharuskan Anda menggunakan Route 53 sebagai penyedia layanan DNS untuk domain yang terdaftar dengan Route 53.)

Proses tersebut bergantung pada apakah Anda saat ini menggunakan domain tersebut:

- Jika domain sedang mendapatkan lalu lintas—misalnya, jika pengguna Anda menggunakan nama domain untuk menelusuri situs web atau mengakses aplikasi web—lihat [Membuat Route 53 sebagai layanan DNS untuk domain yang sedang digunakan](#).
- Jika domain tidak mendapatkan lalu lintas (atau mendapat lalu lintas yang sangat sedikit), lihat [Membuat Route 53 menjadi layanan DNS untuk domain yang tidak aktif](#).

Untuk kedua opsi tersebut, domain Anda akan tetap tersedia selama seluruh proses migrasi. Namun, jika ada masalah, opsi pertama memungkinkan Anda mengembalikan migrasi dengan cepat. Dengan opsi kedua, domain Anda mungkin tidak tersedia selama beberapa hari.

Jika Anda ingin terhubung dengan seorang ahli di AWS, kunjungi [dukungan Penjualan](#).

Membuat Route 53 sebagai layanan DNS untuk domain yang sedang digunakan

Jika Anda ingin memigrasi layanan DNS ke Amazon Route 53 untuk domain yang sedang mendapatkan lalu lintas—misalnya, jika pengguna Anda menggunakan nama domain untuk menelusuri situs web atau mengakses aplikasi web—lakukan prosedur di bagian ini.

Topik

- [Langkah 1: Dapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS saat ini \(opsional tetapi direkomendasikan\)](#)
- [Langkah 2: Membuat zona yang di-hosting](#)
- [Langkah 3: Membuat catatan](#)
- [Langkah 4: Menurunkan pengaturan TTL](#)
- [Langkah 5: \(Jika Anda telah mengonfigurasi DNSSEC\) Menghapus catatan DS dari zona induk](#)
- [Langkah 6: Menunggu TTL lama kedaluwarsa](#)
- [Langkah 7: Memperbarui catatan NS untuk menggunakan server nama Route 53](#)
- [Langkah 8: Memantau lalu lintas untuk domain](#)
- [Langkah 9: Mengembalikan TTL untuk catatan NS ke nilai yang lebih tinggi](#)
- [Langkah 10: Mentransfer pendaftaran domain ke Amazon Route 53](#)
- [Langkah 11: Mengaktifkan kembali penandatanganan DNSSEC \(jika diperlukan\)](#)

Langkah 1: Dapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS saat ini (opsional tetapi direkomendasikan)

Ketika memigrasi layanan DNS dari penyedia lain ke Route 53, Anda mereproduksi konfigurasi DNS Anda saat ini di Route 53. Di Route 53, Anda membuat zona yang di-hosting dengan nama yang sama seperti domain, dan Anda membuat catatan di zona yang di-hosting. Setiap catatan menunjukkan cara Anda ingin merutekan lalu lintas untuk nama domain atau nama subdomain tertentu. Misalnya, ketika seseorang memasukkan nama domain Anda di browser web, apakah Anda ingin lalu lintas diarahkan ke server web di pusat data Anda, ke EC2 instance Amazon, ke CloudFront distribusi, atau ke lokasi lain?

Proses yang Anda gunakan tergantung pada kompleksitas konfigurasi DNS Anda saat ini:

- Jika konfigurasi DNS Anda saat ini sederhana – Jika Anda merutekan lalu lintas internet hanya untuk beberapa subdomain ke sejumlah kecil sumber daya, seperti server web atau bucket Amazon S3, Anda dapat membuat beberapa catatan secara manual di konsol Route 53.
- Jika konfigurasi DNS Anda saat ini lebih kompleks, dan Anda hanya ingin mereproduksi konfigurasi saat ini – Anda dapat menyederhanakan migrasi jika bisa mendapatkan file zona dari penyedia layanan DNS saat ini, dan mengimpor file zona ke Route 53. (Tidak semua penyedia layanan DNS menawarkan file zona.) Ketika Anda mengimpor file zona, Route 53 secara otomatis mereproduksi konfigurasi yang ada dengan membuat catatan yang sesuai di zona yang di-hosting.

Coba tanyakan ke dukungan pelanggan penyedia layanan DNS Anda saat ini tentang cara mendapatkan file zona atau daftar catatan. Untuk informasi tentang format file zona yang diperlukan, lihat [Membuat catatan dengan mengimpor file zona](#).

- Jika konfigurasi DNS Anda saat ini lebih kompleks, dan Anda tertarik dengan fitur perutean Route 53 – Tinjau dokumentasi berikut untuk melihat apakah Anda ingin menggunakan fitur Route 53 yang tidak tersedia dari penyedia layanan DNS lainnya. Jika iya, Anda dapat membuat catatan secara manual, atau Anda dapat mengimpor file zona lalu membuat atau memperbarui catatan nanti:
- [Memilih antara catatan alias dan nonalias](#) menjelaskan keuntungan dari catatan alias Route 53, yang merutekan lalu lintas ke beberapa AWS sumber daya, seperti CloudFront distribusi dan bucket Amazon S3, tanpa biaya.
- [Memilih kebijakan perutean](#) menjelaskan opsi perutean Route 53, misalnya, perutean berdasarkan lokasi pengguna, perutean berdasarkan latensi antara pengguna dan sumber daya, perutean berdasarkan apakah sumber daya Anda sehat, dan perutean ke sumber daya berdasarkan bobot yang Anda tentukan.

 Note

Anda juga dapat mengimpor file zona dan mengubah konfigurasinya nanti untuk memanfaatkan catatan alias dan kebijakan perutean yang kompleks.

Jika Anda tidak bisa mendapatkan file zona atau jika Anda ingin membuat catatan secara manual di Route 53, catatan yang mungkin akan Anda migrasi meliputi:

- Catatan (Alamat) — mengaitkan nama domain atau nama subdomain dengan IPv4 alamat (misalnya, 192.0.2.3) dari sumber daya yang sesuai
- Catatan AAAA (Alamat) — kaitkan nama domain atau nama subdomain dengan IPv6 alamat (misalnya, 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) dari sumber daya yang sesuai
- Catatan server email (MX) – merutekan lalu lintas ke server email
- Catatan CNAME – mengubah rute lalu lintas untuk satu nama domain (example.net) ke nama domain lain (example.com)
- Catatan untuk jenis catatan DNS lain yang didukung – Untuk daftar jeinis catatan yang didukung, lihat [Tipe data DNS yang didukung](#).

Langkah 2: Membuat zona yang di-hosting

Untuk memberi tahu Amazon Route 53 bagaimana Anda ingin merutekan lalu lintas untuk domain Anda, Anda membuat zona yang dihosting yang memiliki nama yang sama dengan domain Anda, lalu Anda membuat catatan di zona yang dihosting.

Important

Anda dapat membuat zona yang di-hosting hanya untuk domain yang izin administrasinya Anda miliki. Biasanya, ini berarti Anda memiliki domain, tetapi Anda mungkin mengembangkan aplikasi untuk pendaftar domain.

Ketika Anda membuat zona yang di-hosting, Route 53 secara otomatis membuat catatan server nama (NS) dan catatan start of authority (SOA) untuk zona. Catatan NS mengidentifikasi empat server nama yang dikaitkan Route 53 dengan zona yang di-hosting. Untuk membuat Route 53 menjadi layanan DNS bagi domain Anda, perbarui pendaftaran domain untuk menggunakan keempat server nama tersebut.

Important

Jangan buat server nama (NS) tambahan atau catatan start of authority (SOA), serta jangan hapus catatan NS dan SOA yang sudah ada.

Cara membuat zona yang di-hosting

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Jika Anda baru mengenal Route 53, pilih Memulai di bawah Manajemen DNS, lalu pilih Buat zona yang di-hosting.

Jika Anda sudah menggunakan Route 53, pilih Zona yang di-hosting pada panel navigasi, lalu pilih Buat zona yang di-hosting.

3. Pada panel Buat zona yang di-hosting, masukkan nama domain dan, secara opsional, komentar. Untuk informasi lebih lanjut tentang pengaturan, pilih untuk membuka panel bantuan di sisi kanan.

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

4. Untuk Jenis, terima nilai default Zona yang di-hosting publik.
5. Pilih Buat zona yang di-hosting.

Langkah 3: Membuat catatan

Setelah membuat zona yang di-hosting, Anda membuat catatan di zona yang di-hosting yang menentukan lokasi tujuan Anda ingin merutekan lalu lintas untuk domain (example.com) atau subdomain (www.example.com). Misalnya, jika Anda ingin merutekan lalu lintas untuk example.com dan www.example.com ke server web pada EC2 instance Amazon, Anda membuat dua catatan, satu bernama example.com dan yang lainnya bernama www.example.com. Di setiap catatan, Anda menentukan alamat IP untuk EC2 instance Anda.

Anda dapat membuat catatan dengan berbagai cara:

Mengimpor file zona

Ini adalah metode termudah jika Anda mendapatkan file zona dari layanan DNS saat ini di [Langkah 1: Dapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS saat ini \(opsional tetapi direkomendasikan\)](#). Amazon Route 53 tidak dapat memprediksi kapan catatan alias harus dibuat atau menggunakan jenis perutean khusus seperti tertimbang atau failover. Sebagai hasilnya, jika Anda mengimpor file zona, Route 53 membuat catatan DNS standar menggunakan kebijakan perutean sederhana.

Untuk informasi selengkapnya, lihat [Membuat catatan dengan mengimpor file zona](#).

Membuat catatan secara individual di konsol

Jika Anda tidak mendapatkan file zona dan hanya ingin membuat beberapa catatan dengan kebijakan perutean Sederhana untuk memulai, Anda dapat membuat catatan di konsol Route 53. Anda dapat membuat catatan alias dan non-alias.

Untuk informasi selengkapnya, lihat topik berikut.

- [Memilih kebijakan perutean](#)
- [Memilih antara catatan alias dan nonalias](#)
- [Membuat catatan dengan menggunakan konsol Amazon Route 53](#)

Membuat catatan secara terprogram

Anda dapat membuat catatan dengan menggunakan salah satu AWS SDKs, AWS CLI, atau AWS Tools for Windows PowerShell. Untuk informasi selengkapnya, lihat [Dokumentasi AWS](#).

Jika Anda menggunakan bahasa pemrograman yang AWS tidak menyediakan SDK, Anda juga dapat menggunakan Route 53 API. Untuk informasi lebih lanjut, lihat [Referensi API Amazon Route 53](#).

Langkah 4: Menurunkan pengaturan TTL

Pengaturan TTL (waktu untuk tayang) bagi catatan menentukan durasi penyelesai DNS untuk meng-cache catatan dan menggunakan informasi yang di-cache. Ketika TTL berakhir, penyelesai mengirimkan kueri lain ke penyedia layanan DNS untuk domain guna mendapatkan informasi terbaru.

Pengaturan TTL khas untuk catatan NS adalah 172800 detik, atau dua hari. Catatan NS mencantumkan server nama yang dapat digunakan Sistem Nama Domain (DNS) untuk mendapatkan informasi tentang cara merutekan lalu lintas domain Anda. Menurunkan TTL untuk catatan NS, baik dengan penyedia layanan DNS Anda saat ini maupun dengan Amazon Route 53, mengurangi waktu henti untuk domain Anda jika Anda menemukan masalah saat Anda memigrasikan DNS ke Route 53. Jika Anda tidak menurunkan TTL, domain mungkin tidak tersedia di internet hingga dua hari jika terjadi kesalahan.

Note

Beberapa resolver penuh dapat menyimpan TTL dari catatan NS dari server otoritatif induk, oleh karena itu TTL catatan NS yang terdaftar di server DNS otoritatif induk juga harus dikurangi.

Kami merekomendasikan Anda mengubah TTL pada catatan NS berikut:

- Pada catatan NS di zona yang di-hosting untuk penyedia layanan DNS saat ini. (Penyedia Anda saat ini mungkin menggunakan terminologi yang berbeda.)
- Pada catatan NS di zona yang di-hosting yang Anda buat di [Langkah 2: Membuat zona yang di-hosting](#).

Cara menurunkan pengaturan TTL pada catatan NS dengan penyedia layanan DNS saat ini

- Gunakan metode yang disediakan oleh penyedia layanan DNS untuk domain saat ini guna mengubah TTL bagi catatan NS di zona yang di-hosting untuk domain Anda.

Cara menurunkan pengaturan TTL pada catatan NS di zona yang di-hosting Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pilih Zona yang di-hosting di panel navigasi.
3. Pilih nama zona yang di-hosting.
4. Pilih catatan NS, dan pilih Edit.
5. Mengubah nilai TTL (Detik). Kami rekomendasikan Anda menentukan nilai antara 60 detik hingga 900 detik (15 menit).
6. Pilih Simpan perubahan.

Langkah 5: (Jika Anda telah mengonfigurasi DNSSEC) Menghapus catatan DS dari zona induk

Jika Anda telah mengonfigurasi DNSSEC untuk domain, hapus catatan Delegation Signer (DS) dari zona induk sebelum memigrasi domain ke Route 53.

Jika zona induk di-host melalui Route 53 atau registrar lain, hubungi mereka untuk menghapus catatan DS.

Karena saat ini tidak mungkin untuk mengaktifkan penandatanganan DNSSEC di dua penyedia, Anda harus menghapus DS apa pun atau DNSKEYs menonaktifkan DNSSEC. Hal ini memberi sinyal sementara ke penyelesai DNS untuk menonaktifkan validasi DNSSEC. Di [Langkah 11](#), Anda dapat mengaktifkan kembali validasi DNSSEC, jika ingin, setelah transisi ke Route 53 selesai.

Untuk informasi selengkapnya, lihat [Menghapus kunci publik untuk domain](#).

Langkah 6: Menunggu TTL lama kedaluwarsa

Jika domain Anda sedang digunakan—misalnya, jika pengguna menggunakan nama domain untuk menelusuri situs web atau mengakses aplikasi web—penyelesai DNS telah meng-cache nama server nama yang disediakan oleh penyedia layanan DNS Anda saat ini. Penyelesai DNS yang meng-cache informasi tersebut beberapa menit lalu akan menyimpannya selama hampir dua hari.

Untuk memastikan bahwa semua migrasi layanan DNS ke Route 53 terjadi di satu waktu, tunggu selama dua hari setelah Anda menurunkan TTL. Setelah TTL dua hari kedaluwarsa dan penyelesaian meminta server nama untuk domain Anda, penyelesaian akan mendapatkan server nama saat ini dan juga akan mendapatkan TTL baru yang Anda tentukan di [Langkah 4: Menurunkan pengaturan TTL](#).

Langkah 7: Memperbarui catatan NS untuk menggunakan server nama Route 53

Untuk mulai menggunakan Amazon Route 53 sebagai layanan DNS untuk domain, gunakan metode yang disediakan oleh registrar, atau zona induk, untuk menggantikan server nama saat ini dalam catatan NS dengan server nama Route 53.

Note

Ketika memperbarui catatan NS dengan penyedia layanan DNS saat ini untuk menggunakan server nama Route 53, Anda memperbarui konfigurasi DNS untuk domain. (Hal ini sebanding dengan memperbarui catatan NS di zona yang di-hosting Route 53 untuk domain kecuali Anda memperbarui pengaturan dengan layanan DNS tempat asal migrasi.)

Cara memperbarui catatan NS di registrar, atau zona induk, untuk menggunakan server nama Route 53

1. Di konsol Route 53, dapatkan server nama untuk zona yang di-hosting:
 - a. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 - b. Pada panel navigasi, pilih Zona yang di-hosting.
 - c. Pada halaman Zona yang di-hosting, pilih nama zona yang di-hosting yang ada.
 - d. Catat empat nama yang tercantum untuk Server nama di bagian Detail zona yang di-hosting.
2. Gunakan metode yang disediakan oleh penyedia layanan DNS untuk domain saat ini guna memperbarui catatan NS bagi zona yang di-hosting. Jika domain terdaftar dengan Route 53, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#). Proses ini tergantung pada apakah layanan DNS saat ini mengizinkan Anda menghapus server nama:

Jika Anda dapat menghapus server nama

- Catat nama server nama saat ini dalam catatan NS untuk zona yang di-hosting. Jika Anda perlu kembali ke konfigurasi DNS saat ini, berikut adalah server yang akan Anda tentukan.
- Hapus server nama saat ini dari catatan NS.
- Perbarui catatan NS dengan nama keempat server nama Route 53 yang Anda dapatkan di langkah 1 dari prosedur ini.

 Note

Setelah selesai, satu-satunya server nama dalam catatan NS adalah keempat server nama Route 53 tersebut.

Jika Anda tidak dapat menghapus server nama

- Pilih opsi untuk menggunakan server nama kustom.
- Tambahkan keempat server nama Route 53 yang Anda dapatkan di langkah 1 prosedur ini.

Langkah 8: Memantau lalu lintas untuk domain

Memantau lalu lintas untuk domain, termasuk lalu lintas situs web atau aplikasi, dan email:

- Jika lalu lintas melambat atau berhenti – Gunakan metode yang disediakan oleh layanan DNS sebelumnya guna mengembalikan server nama untuk domain ke server nama sebelumnya. Ini adalah server nama yang Anda catat di langkah 7 pada [Cara memperbarui catatan NS di registrar, atau zona induk, untuk menggunakan server nama Route 53](#). Kemudian tentukan apa yang salah.
- Jika lalu lintas tidak terpengaruh – Lanjutkan ke [Langkah 9: Mengembalikan TTL untuk catatan NS ke nilai yang lebih tinggi](#).

Langkah 9: Mengembalikan TTL untuk catatan NS ke nilai yang lebih tinggi

Di zona yang di-hosting untuk domain Amazon Route 53, ubah TTL untuk catatan NS menjadi nilai yang lebih khas, misalnya 172800 detik (dua hari). Hal ini meningkatkan latensi untuk pengguna Anda karena mereka tidak harus sering menunggu penyelesaian DNS mengirim kueri bagi server nama untuk domain Anda.

Cara mengubah TTL untuk catatan NS di zona yang di-hosting Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pilih Zona yang di-hosting di panel navigasi.
3. Pilih nama zona yang di-hosting.
4. Dalam daftar catatan untuk zona yang di-hosting, pilih catatan NS.
5. Pilih Edit.
6. Ubah TTL (detik) menjadi jumlah detik yang Anda inginkan bagi penyelesaian DNS meng-cache nama server nama untuk domain Anda. Kami merekomendasikan nilai 172800 detik.
7. Pilih Simpan perubahan.

Langkah 10: Mentransfer pendaftaran domain ke Amazon Route 53

Sekarang setelah Anda mentransfer layanan DNS untuk domain ke Amazon Route 53, Anda dapat mentransfer pendaftaran domain ke Route 53 secara opsional. Untuk informasi selengkapnya, lihat [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#).

Langkah 11: Mengaktifkan kembali penandatanganan DNSSEC (jika diperlukan)

Setelah mentransfer layanan DNS untuk domain ke Amazon Route 53, Anda dapat mengaktifkan kembali penandatanganan DNSSEC.

Ada dua langkah untuk mengaktifkan penandatanganan DNSSEC:

- Langkah 1: Aktifkan penandatanganan DNSSEC untuk Route 53, dan minta Route 53 membuat kunci penandatanganan kunci (KSK) berdasarkan kunci yang dikelola pelanggan di AWS Key Management Service (KMS).
- Langkah 2: Membuat rantai kepercayaan untuk zona yang di-hosting dengan menambahkan catatan Delegation Signer (DS) ke zona induk, sehingga respons DNS dapat diautentikasi dengan tanda tangan kriptografi terpercaya.

Untuk petunjuk, silakan lihat [Mengaktifkan penandatanganan DNSSEC dan membuat rantai kepercayaan](#).

Membuat Route 53 menjadi layanan DNS untuk domain yang tidak aktif

Jika Anda ingin memigrasi layanan DNS ke Amazon Route 53 untuk domain yang tidak mendapatkan lalu lintas (atau mendapatkan sangat sedikit lalu lintas), lakukan prosedur di bagian ini.

Topik

- [Langkah 1: Dapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS saat ini \(domain yang tidak aktif\)](#)
- [Langkah 2: Membuat zona yang di-hosting \(domain tidak aktif\)](#)
- [Langkah 3: Membuat catatan \(domain yang tidak aktif\)](#)
- [Langkah 4: Memperbarui pendaftaran domain untuk menggunakan server nama Amazon Route 53 \(domain yang tidak aktif\)](#)

Langkah 1: Dapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS saat ini (domain yang tidak aktif)

Ketika memigrasi layanan DNS dari penyedia lain ke Route 53, Anda mereproduksi konfigurasi DNS Anda saat ini di Route 53. Di Route 53, Anda membuat zona yang di-hosting dengan nama yang sama seperti domain, dan Anda membuat catatan di zona yang di-hosting. Setiap catatan menunjukkan cara Anda ingin merutekan lalu lintas untuk nama domain atau nama subdomain tertentu. Misalnya, ketika seseorang memasukkan nama domain Anda di browser web, apakah Anda ingin lalu lintas diarahkan ke server web di pusat data Anda, ke EC2 instance Amazon, ke CloudFront distribusi, atau ke lokasi lain?

Proses yang Anda gunakan tergantung pada kompleksitas konfigurasi DNS Anda saat ini:

- Jika konfigurasi DNS Anda saat ini sederhana – Jika Anda merutekan lalu lintas internet hanya untuk beberapa subdomain ke sejumlah kecil sumber daya, seperti server web atau bucket Amazon S3, Anda dapat membuat beberapa catatan secara manual di konsol Route 53.
- Jika konfigurasi DNS Anda saat ini lebih kompleks, dan Anda hanya ingin mereproduksi konfigurasi saat ini – Anda dapat menyederhanakan migrasi jika bisa mendapatkan file zona dari penyedia layanan DNS saat ini, dan mengimpor file zona ke Route 53. (Tidak semua penyedia layanan DNS menawarkan file zona.) Ketika Anda mengimpor file zona, Route 53 secara otomatis mereproduksi konfigurasi yang ada dengan membuat catatan yang sesuai di zona yang di-hosting.

Coba tanyakan ke dukungan pelanggan penyedia layanan DNS Anda saat ini tentang cara mendapatkan file zona atau daftar catatan. Untuk informasi tentang format file zona yang diperlukan, lihat [Membuat catatan dengan mengimpor file zona](#).

- Jika konfigurasi DNS Anda saat ini lebih kompleks, dan Anda tertarik dengan fitur perutean Route 53 – Tinjau dokumentasi berikut untuk melihat apakah Anda ingin menggunakan fitur Route 53 yang tidak tersedia dari penyedia layanan DNS lainnya. Jika iya, Anda dapat membuat catatan secara manual, atau Anda dapat mengimpor file zona lalu membuat atau memperbarui catatan nanti:
- [Memilih antara catatan alias dan nonalias](#) menjelaskan keuntungan dari catatan alias Route 53, yang merutekan lalu lintas ke beberapa AWS sumber daya, seperti CloudFront distribusi dan bucket Amazon S3, tanpa biaya.
- [Memilih kebijakan perutean](#) menjelaskan opsi perutean Route 53, misalnya, perutean berdasarkan lokasi pengguna, perutean berdasarkan latensi antara pengguna dan sumber daya, perutean berdasarkan apakah sumber daya Anda sehat, dan perutean ke sumber daya berdasarkan bobot yang Anda tentukan.

 Note

Anda juga dapat mengimpor file zona dan mengubah konfigurasinya nanti untuk memanfaatkan catatan alias dan kebijakan perutean yang kompleks.

Jika Anda tidak bisa mendapatkan file zona atau jika Anda ingin membuat catatan secara manual di Route 53, catatan yang mungkin akan Anda migrasi meliputi:

- Catatan (Alamat) — mengaitkan nama domain atau nama subdomain dengan IPv4 alamat (misalnya, 192.0.2.3) dari sumber daya yang sesuai
- Catatan AAAA (Alamat) — kaitkan nama domain atau nama subdomain dengan IPv6 alamat (misalnya, 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) dari sumber daya yang sesuai
- Catatan server email (MX) – merutekan lalu lintas ke server email
- Catatan CNAME – mengubah rute lalu lintas untuk satu nama domain (example.net) ke nama domain lain (example.com)
- Catatan untuk jenis catatan DNS lain yang didukung – Untuk daftar jeinis catatan yang didukung, lihat [Tipe data DNS yang didukung](#).

Langkah 2: Membuat zona yang di-hosting (domain tidak aktif)

Untuk memberi tahu Amazon Route 53 bagaimana Anda ingin merutekan lalu lintas untuk domain Anda, Anda membuat zona yang dihosting yang memiliki nama yang sama dengan domain Anda, lalu Anda membuat catatan di zona yang dihosting.

Important

Anda dapat membuat zona yang di-hosting hanya untuk domain yang izin administrasinya Anda miliki. Biasanya, ini berarti Anda memiliki domain, tetapi Anda mungkin mengembangkan aplikasi untuk pendaftar domain.

Ketika Anda membuat zona yang di-hosting, Route 53 secara otomatis membuat catatan server nama (NS) dan catatan start of authority (SOA) untuk zona. Catatan NS mengidentifikasi empat server nama yang dikaitkan Route 53 dengan zona yang di-hosting. Untuk membuat Route 53 menjadi layanan DNS bagi domain Anda, perbarui pendaftaran domain untuk menggunakan keempat server nama tersebut.

Important

Jangan buat server nama (NS) tambahan atau catatan start of authority (SOA), serta jangan hapus catatan NS dan SOA yang sudah ada.

Cara membuat zona yang di-hosting

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Jika Anda baru mengenal Route 53, pilih Memulai.

Jika Anda sudah menggunakan Route 53, pilih Zona yang di-hosting pada panel navigasi.

3. Pilih Buat zona yang di-hosting.
4. Pada panel Buat zona yang di-hosting, masukkan nama domain dan, secara opsional, komentar. Untuk informasi lebih lanjut tentang pengaturan, posisikan penunjuk mouse di atas labelnya untuk melihat kiat alat.

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

5. Untuk Jenis catatan, terima nilai default zona yang di-hosting secara publik.
6. Pilih Buat zona yang di-hosting.

Langkah 3: Membuat catatan (domain yang tidak aktif)

Setelah membuat zona yang di-hosting, Anda membuat catatan di zona yang di-hosting yang menentukan lokasi tujuan Anda ingin merutekan lalu lintas untuk domain (example.com) atau subdomain (www.example.com). Misalnya, jika Anda ingin merutekan lalu lintas untuk example.com dan www.example.com ke server web pada EC2 instance Amazon, Anda membuat dua catatan, satu bernama example.com dan yang lainnya bernama www.example.com. Di setiap catatan, Anda menentukan alamat IP untuk EC2 instance Anda.

Anda dapat membuat catatan dengan berbagai cara:

Mengimpor file zona

Ini adalah metode termudah jika Anda mendapatkan file zona dari layanan DNS saat ini di [Langkah 1: Dapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS saat ini \(domain yang tidak aktif\)](#). Amazon Route 53 tidak dapat memprediksi kapan catatan alias harus dibuat atau menggunakan jenis perutean khusus seperti tertimbang atau failover. Sebagai hasilnya, jika Anda mengimpor file zona, Route 53 membuat catatan DNS standar menggunakan kebijakan perutean sederhana.

Untuk informasi selengkapnya, lihat [Membuat catatan dengan mengimpor file zona](#).

Membuat catatan secara individual di konsol

Jika Anda tidak mendapatkan file zona dan hanya ingin membuat beberapa catatan dengan kebijakan perutean Sederhana untuk memulai, Anda dapat membuat catatan di konsol Route 53. Anda dapat membuat catatan alias dan non-alias.

Untuk informasi selengkapnya, lihat topik berikut.

- [Memilih kebijakan perutean](#)
- [Memilih antara catatan alias dan nonalias](#)
- [Membuat catatan dengan menggunakan konsol Amazon Route 53](#)

Membuat catatan secara terprogram

Anda dapat membuat catatan dengan menggunakan salah satu AWS SDKs, AWS CLI, atau AWS Tools for Windows PowerShell. Untuk informasi selengkapnya, lihat [Dokumentasi AWS](#).

Jika Anda menggunakan bahasa pemrograman yang AWS tidak menyediakan SDK, Anda juga dapat menggunakan Route 53 API. Untuk informasi lebih lanjut, lihat [Referensi API Amazon Route 53](#).

Langkah 4: Memperbarui pendaftaran domain untuk menggunakan server nama Amazon Route 53 (domain yang tidak aktif)

Setelah selesai membuat catatan untuk domain, Anda dapat mengubah layanan DNS untuk domain Anda menjadi Amazon Route 53. Lakukan prosedur berikut untuk memperbarui pengaturan dengan registrar domain.

Cara memperbarui server nama untuk domain

1. Di konsol Route 53, dapatkan server nama untuk zona yang di-hosting Route 53:
 - a. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 - b. Pada panel navigasi, pilih Zona yang di-hosting.
 - c. Pada halaman Zona yang di-hosting, pilih tombol radio (bukan nama) untuk zona yang di-hosting, lalu pilih Lihat detail.
 - d. Pada halaman detail untuk zona yang di-hosting, pilih Detail zona yang di-hosting.
 - e. Catat empat server yang tercantum untuk Server nama.
2. Gunakan metode yang disediakan oleh registrar untuk domain untuk mengubah server nama domain untuk menggunakan empat server nama Route 53 yang Anda dapatkan di langkah 2 dari prosedur ini.

Jika domain terdaftar dengan Route 53, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

Mengonfigurasi perutean DNS untuk domain baru

Domain baru yang Anda beli dari Route 53

Saat Anda mendaftarkan domain dengan Route 53, secara otomatis kami menjadikan Route 53 sebagai layanan DNS untuk domain tersebut. Route 53 menciptakan zona yang di-hosting dengan nama yang sama seperti domain, menetapkan empat server nama untuk zona yang di-hosting, dan memperbarui domain untuk menggunakan server nama tersebut.

Domain baru yang Anda beli dari registrar lain

Ketika Anda membeli domain dari registrar lain, misalnya, karena domain tingkat atas (TLD) tidak ditawarkan oleh Route 53, Anda memiliki dua opsi:

- Gunakan Route 53 hanya untuk hosting DNS: Simpan registrar Anda saat ini tetapi delegasikan manajemen DNS ke Route 53. Ikuti prosedur di bawah ini untuk membuat zona yang dihosting dan memperbarui server nama registrar Anda.
- Transfer pendaftaran domain ke Route 53: Jadikan Route 53 sebagai registrar dan layanan DNS Anda. Lihat [Daftar periksa pra-transfer untuk transfer domain](#) prasyarat dan [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#) untuk proses transfer.

Untuk informasi selengkapnya tentang TLDs didukung oleh Route 53, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Ikuti petunjuk ini untuk membuat zona yang dihosting publik dan kemudian gunakan server nama yang dibuat dengan registrar:

Untuk membuat zona yang dihosting untuk domain non-Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang di-hosting, lalu pilih Buat zona yang di-hosting.
3. Untuk Nama, masukkan nama domain yang ingin Anda buat zona yang dihosting, seperti deskripsi opsional `example.com`, pilih Zona yang dihosting publik, lalu Buat zona yang dihosting.
4. Setelah Anda membuat zona yang dihosting, perhatikan empat catatan server nama (NS) yang dibuat. Masing-masing akan dimulai dengan “ns-”.

Di registrar domain Anda, masukkan server nama dari atas untuk mendelegasikan manajemen domain ke zona host Route 53 Anda.

Rute lalu lintas DNS

Untuk menentukan bagaimana Anda ingin Route 53 untuk merutekan lalu lintas internet untuk domain, Anda membuat catatan di zona yang dihosting. Misalnya, jika Anda ingin merutekan permintaan example.com ke server web yang berjalan di EC2 instance Amazon, Anda membuat catatan di zona yang dihosting example.com, dan Anda menentukan alamat IP Elastis untuk instance tersebut. Untuk informasi selengkapnya, lihat topik berikut:

- Untuk informasi tentang cara membuat catatan di zona yang di-hosting, lihat [Bekerja dengan catatan](#).
- Untuk informasi tentang cara merutekan lalu lintas ke AWS sumber daya yang dipilih, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).
- Untuk informasi selengkapnya tentang cara kerja DNS, lihat [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#).
- Untuk memeriksa DNS response, lihat [Memeriksa respons DNS dari Route 53](#)

Merutekan lalu lintas ke sumber daya

Ketika pengguna meminta situs web atau aplikasi web Anda, misalnya, dengan memasukkan nama domain Anda di browser web, Amazon Route 53 membantu mengarahkan pengguna ke sumber daya Anda, seperti bucket Amazon S3 atau server web di pusat data Anda. Untuk mengonfigurasi Route 53 untuk merutekan lalu lintas ke sumber daya Anda, Anda melakukan hal berikut:

1. Membuat zona yang di-hosting. Anda dapat membuat zona yang di-hosting secara publik atau zona yang di-hosting secara privat:

Zona yang di-hosting secara publik

Buat zona yang di-hosting secara publik jika Anda ingin merutekan lalu lintas internet ke sumber daya, misalnya, agar pelanggan Anda dapat melihat situs web perusahaan yang Anda host di instance EC2. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting publik](#).

Zona yang di-hosting secara privat

Buat zona yang di-hosting secara privat jika Anda ingin merutekan lalu lintas di dalam Amazon VPC. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting privat](#).

2. Membuat catatan di zona yang di-hosting. Catatan menentukan tujuan perutean lalu lintas untuk setiap nama domain atau nama subdomain. Misalnya, untuk merutekan lalu

lintas `www.example.com` ke server web di pusat data, Anda biasanya membuat catatan `www.example.com` di zona yang di-hosting `example.com`.

Untuk informasi selengkapnya, lihat topik berikut:

- [Bekerja dengan catatan](#)
- [Merutekan lalu lintas untuk subdomain](#)
- [Merutekan lalu lintas internet ke sumber daya Anda AWS](#)

Merutekan lalu lintas untuk subdomain

Jika ingin merutekan lalu lintas subdomain ke sumber daya, seperti `acme.example.com` atau `zenith.example.com`, Anda memiliki dua opsi:

Membuat catatan di zona yang di-hosting untuk domain

Biasanya, untuk merutekan lalu lintas subdomain, Anda membuat catatan di zona yang di-hosting yang memiliki nama yang sama seperti domain. Misalnya, untuk merutekan lalu lintas internet `acme.example.com` ke server web di pusat data, Anda membuat catatan bernama `acme.example.com` dalam zona yang di-hosting `example.com`. Untuk informasi selengkapnya, lihat topik [Bekerja dengan catatan](#) dan subtopiknya.

Membuat zona yang di-hosting untuk subdomain, dan membuat catatan di zona yang di-hosting baru

Anda juga dapat membuat zona yang di-hosting untuk subdomain. Menggunakan zona yang di-hosting terpisah untuk merutekan lalu lintas internet bagi subdomain terkadang dikenal sebagai "mendelegasikan tanggung jawab untuk subdomain ke zona yang di-hosting" atau "mendelegasikan subdomain ke server nama lain" atau beberapa kombinasi istilah yang serupa. Berikut adalah gambaran umum cara kerjanya:

1. Anda membuat zona yang di-hosting dengan nama yang sama seperti subdomain yang lalu lintasnya ingin Anda rutekan, seperti `acme.example.com`.
2. Anda membuat catatan di zona yang di-hosting baru yang menentukan cara Anda ingin merutekan lalu lintas untuk subdomain (`acme.example.com`) dan subdomain-nya, seperti `backend.acme.example.com`.
3. Anda mendapatkan server nama yang ditetapkan Route 53 ke zona yang di-hosting baru ketika Anda membuatnya.

4. Anda membuat catatan NS baru di zona yang dihosting untuk domain (example.com). Nama catatan NS harus nama subdomain (acme.example.com), dan Anda menentukan empat server nama yang Anda dapatkan di langkah 3 sebagai nilai catatan.

Ketika menggunakan zona yang di-hosting terpisah untuk merutekan lalu lintas subdomain, Anda dapat menggunakan izin IAM untuk membatasi akses ke zona yang di-hosting bagi subdomain. Jika Anda memiliki beberapa subdomain yang dikelola oleh grup yang berbeda, membuat zona yang di-hosting untuk setiap subdomain secara signifikan dapat mengurangi jumlah orang yang harus memiliki akses ke catatan dalam zona yang di-hosting untuk domain.

Untuk mengimplementasikan proses delegasi ini, Anda memerlukan izin IAM berikut. Untuk informasi selengkapnya tentang kebijakan IAM Route 53, lihat [Identity and access management di Amazon Route 53](#):

Akun induk (memiliki example.com)

Pengguna atau peran memerlukan izin untuk mengubah catatan di zona host domain induk:

Akun anak (membuat acme.example.com)

Pengguna atau peran memerlukan izin untuk membuat dan mengelola zona host subdomain:

Menggunakan zona yang di-hosting terpisah untuk subdomain juga memungkinkan Anda menggunakan layanan DNS yang berbeda bagi domain dan subdomain. Untuk informasi selengkapnya, lihat [Menggunakan Amazon Route 53 sebagai layanan DNS untuk subdomain tanpa memigrasi domain induk](#).

Ada dampak kecil pada performa untuk konfigurasi ini bagi kueri DNS pertama dari setiap penyelesai DNS. Penyelesai harus mendapatkan informasi dari zona yang di-hosting bagi domain root lalu mendapatkan informasi dari zona yang di-hosting untuk subdomain. Setelah kueri DNS pertama untuk subdomain, penyelesai meng-cache informasi dan tidak perlu mendapatkannya lagi hingga TTL berakhir dan klien lain meminta subdomain dari penyelesai tersebut. Untuk informasi selengkapnya, lihat [TTL \(detik\)](#) di bagian [Nilai yang Anda tentukan saat membuat atau mengedit catatan Amazon Route 53](#).

Topik

- [Membuat zona yang di-hosting lainnya untuk merutekan lalu lintas bagi subdomain](#)
- [Merutekan lalu lintas untuk tingkat subdomain tambahan](#)

Membuat zona yang di-hosting lainnya untuk merutekan lalu lintas bagi subdomain

Cara merutekan lalu lintas untuk subdomain adalah membuat zona yang di-hosting untuk subdomain, lalu membuat catatan untuk subdomain di zona yang di-hosting baru. (Opsional yang lebih umum adalah membuat catatan untuk subdomain di zona yang di-hosting untuk domain.)

Note

Prosedur ini menunjukkan cara mendelegasikan subdomain ke Route 53. Anda juga dapat mendelegasikan subdomain ke layanan DNS lain dengan membuat catatan NS yang mengarah ke server nama layanan tersebut.

Berikut adalah gambaran umum prosesnya:

1. Membuat zona yang di-hosting untuk subdomain. Untuk informasi selengkapnya, lihat [Membuat zona yang di-hosting baru untuk subdomain](#).
2. Menambahkan catatan ke zona yang di-hosting untuk subdomain. Jika zona yang di-hosting untuk domain berisi catatan yang merupakan bagian dari zona yang di-hosting untuk subdomain, duplikatkan catatan tersebut di zona yang di-hosting untuk subdomain. Untuk informasi selengkapnya, lihat [Membuat catatan di zona yang di-hosting untuk subdomain](#).
3. Membuat catatan NS untuk subdomain di zona yang di-hosting untuk domain, yang mendelegasikan tanggung jawab untuk subdomain ke server nama di zona yang di-hosting baru. Jika zona yang di-hosting untuk domain berisi catatan yang merupakan bagian dari zona yang di-hosting untuk subdomain, hapus catatan tersebut dari zona yang di-hosting untuk subdomain. (Anda membuat salinan di zona yang di-hosting untuk subdomain di langkah 2.) Untuk informasi selengkapnya, lihat [Memperbarui zona yang di-hosting untuk domain](#).

Membuat zona yang di-hosting baru untuk subdomain

Untuk membuat zona yang di-hosting bagi subdomain menggunakan konsol Route 53, lakukan prosedur berikut.

Cara membuat zona yang di-hosting untuk subdomain (konsol)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Jika Anda baru mengenal Route 53, pilih Memulai.

Jika Anda sudah menggunakan Route 53, pilih Zona yang di-hosting pada panel navigasi.

3. Pilih Buat zona yang di-hosting.
4. Di panel kanan, masukkan nama subdomain, seperti `acme.example.com`. Secara opsional Anda juga dapat memasukkan komentar.

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

5. Untuk Jenis, terima nilai default Zona yang di-hosting publik.
6. Di bagian bawah panel kanan, pilih Buat zona yang di-hosting.

Membuat catatan di zona yang di-hosting untuk subdomain

Untuk menentukan bagaimana Anda ingin Route 53 untuk merutekan lalu lintas untuk subdomain (`acme.example.com`) dan subdomainnya (`backend.acme.example.com`), Anda membuat catatan di zona yang dihosting untuk subdomain.

Perhatikan penjelasan berikut tentang membuat catatan di zona yang di-hosting untuk subdomain:

- Jangan buat server nama (NS) tambahan atau catatan start of authority (SOA) di zona yang di-hosting untuk subdomain, serta jangan hapus catatan NS dan SOA yang sudah ada.
- Buat semua catatan untuk subdomain di dalam zona yang di-hosting untuk subdomain. Misalnya, jika Anda memiliki zona yang di-hosting untuk `example.com` dan domain `acme.example.com`, buat semua catatan untuk subdomain `acme.example.com` di zona yang di-hosting `acme.example.com`. Ini termasuk catatan seperti `backend.acme.example.com` dan `beta.backend.acme.example.com`.
- Jika zona yang di-hosting untuk domain (`example.com`) telah berisi catatan yang merupakan bagian dari zona yang di-hosting untuk subdomain (`acme.example.com`), duplikatkan catatan tersebut di zona yang di-hosting untuk subdomain. Pada langkah terakhir dari proses, Anda menghapus data duplikat dari zona yang di-hosting untuk domain.

Important

Jika Anda memiliki beberapa catatan untuk subdomain di zona yang di-hosting domain dan zona yang di-hosting untuk subdomain, perilaku DNS akan menjadi tidak konsisten. Perilaku akan tergantung pada server nama penyelesai DNS yang telah di-cache, server nama untuk zona yang di-hosting domain (`example.com`) atau server nama untuk zona yang di-hosting subdomain (`acme.example.com`). Dalam beberapa kasus, Route 53 akan

mengembalikan NXDOMAIN (tidak ada domain) ketika catatan ada, tetapi tidak di zona yang di-hosting yang menjadi tujuan kueri yang dikirimkan oleh penyelesai DNS.

Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).

Memperbarui zona yang di-hosting untuk domain

Saat Anda membuat zona yang di-hosting, Route 53 secara otomatis menetapkan empat server nama ke zona. Catatan NS untuk zona yang di-hosting mengidentifikasi server nama yang merespons kueri DNS bagi domain atau subdomain. Untuk mulai menggunakan catatan di zona yang di-hosting bagi subdomain guna merutekan lalu lintas internet, Anda membuat catatan NS baru di zona yang di-hosting untuk domain (example.com), dan memberinya nama subdomain (acme.example.com). Untuk nilai catatan NS, Anda menentukan nama untuk server nama dari zona yang di-hosting bagi subdomain.

Ini adalah yang terjadi jika Route 53 menerima kueri DNS dari penyelesai DNS untuk subdomain acme.example.com atau salah satu subdomainnya:

1. Route 53 terlihat di zona yang di-hosting untuk domain (example.com) dan menemukan catatan NS untuk subdomain (acme.example.com).
2. Route 53 mendapatkan server nama dari catatan NS acme.example.com di zona yang di-hosting untuk domain, example.com, dan mengembalikan server nama ke penyelesai DNS.
3. Penyelesai mengirimkan ulang kueri untuk acme.example.com ke server nama untuk zona yang di-hosting acme.example.com.
4. Route 53 merespons kueri menggunakan catatan dalam zona yang di-hosting acme.example.com.

Untuk mengonfigurasi Route 53 untuk merutekan lalu lintas untuk subdomain menggunakan zona yang dihosting untuk subdomain dan untuk menghapus catatan duplikat apa pun dari zona yang dihosting untuk domain, lakukan prosedur berikut:

Untuk mengonfigurasi Route 53 agar menggunakan zona yang di-hosting bagi subdomain (konsol)

1. Di konsol Route 53, dapatkan server nama untuk zona yang di-hosting bagi subdomain:
 - a. Pada panel navigasi, pilih Zona yang di-hosting.
 - b. Pada halaman Zona yang di-hosting, pilih nama zona yang di-hosting untuk subdomain.

- c. Pada panel kanan, salin nama dari empat server yang terdaftar untuk Server nama di bagian Detail zona yang di-hosting.
2. Pilih nama zona yang di-hosting untuk domain (example.com), bukan untuk subdomain.
3. Pilih Buat catatan.
4. Pilih Perutean sederhana, dan pilih Selanjutnya.
5. Pilih Tentukan catatan sederhana.
6. Tentukan nilai-nilai berikut ini:

Nama

Masukkan nama subdomain (misalnya, `acme.example.com`). Ini harus sama persis dengan nama zona host subdomain yang Anda buat.

Nilai/Rutekan lalu lintas ke

Pilih alamat IP atau nilai lain tergantung pada jenis catatan, dan tempel nama-nama server nama yang Anda salin di langkah 1.

Jenis catatan

Pilih NS – Server nama untuk zona yang di-hosting.

TTL (Detik)

Ubah ke nilai yang lebih umum untuk catatan NS, seperti 172800 detik.

7. Pilih Tentukan catatan sederhana, dan pilih Buat catatan.
8. Jika zona yang di-hosting untuk domain berisi catatan yang Anda buat ulang di zona yang di-hosting untuk subdomain, hapus catatan tersebut dari zona yang di-hosting untuk subdomain. Untuk informasi selengkapnya, lihat [Menghapus catatan](#).

Setelah Anda selesai, semua catatan untuk subdomain seharusnya berada di dalam zona yang di-hosting untuk subdomain.

Merutekan lalu lintas untuk tingkat subdomain tambahan

Anda merutekan lalu lintas ke subdomain dari subdomain, seperti `backend.acme.example.com`, dengan cara yang sama seperti merutekan lalu lintas ke subdomain, seperti `acme.example.com`. Baik Anda membuat catatan di zona yang di-hosting untuk domain, atau membuat zona yang di-hosting untuk subdomain tingkat yang lebih rendah, lalu membuat catatan di zona yang di-hosting baru.

Jika Anda memilih untuk membuat zona yang di-hosting terpisah untuk subdomain tingkat yang lebih rendah, buat catatan NS untuk subdomain tingkat yang lebih rendah di zona yang di-hosting untuk subdomain yang satu tingkat lebih dekat dengan nama domain. Tindakan ini membantu memastikan bahwa lalu lintas dirutekan dengan benar ke sumber daya Anda. Sebagai contoh, Anda ingin merutekan lalu lintas untuk subdomain berikut:

- subdomain1.example.com
- subdomain2.subdomain1.example.com

Untuk menggunakan zona yang di-hosting lainnya guna merutekan lalu lintas bagi subdomain2.subdomain1.example.com, lakukan hal berikut:

1. Membuat zona yang di-hosting bernama subdomain2.subdomain1.example.com.
2. Membuat catatan di zona yang di-hosting subdomain2.subdomain1.example.com. Untuk informasi selengkapnya, lihat [Membuat catatan di zona yang di-hosting untuk subdomain](#).
3. Salin nama server nama untuk zona yang di-hosting subdomain2.subdomain1.example.com.
4. Di zona yang di-hosting subdomain1.example.com, buat catatan NS bernama subdomain2.subdomain1.example.com, dan tempel nama server nama untuk zona yang di-hosting subdomain2.subdomain1.example.com.

Selain itu, hapus data duplikat dari subdomain1.example.com. Untuk informasi selengkapnya, lihat [Memperbarui zona yang di-hosting untuk domain](#).

Setelah Anda membuat catatan NS ini, Route 53 mulai menggunakan zona host subdomain2.subdomain1.example.com untuk merutekan lalu lintas subdomain2.subdomain1.example.com subdomain.

Bekerja dengan zona yang di-hosting

Zona yang di-hosting adalah kontainer untuk catatan, dan catatan berisi informasi tentang cara merutekan lalu lintas untuk domain tertentu, seperti example.com, dan subdomainnya (acme.example.com, zenith.example.com). Zona yang di-hosting dan domain yang sesuai memiliki nama yang sama. Ada dua tipe zona yang di-hosting:

- Zona yang di-hosting publik berisi catatan yang menentukan bagaimana Anda ingin merutekan lalu lintas di internet. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting publik](#).

- Zona yang di-hosting publik berisi catatan yang menentukan bagaimana Anda ingin merutekan lalu lintas di Amazon VPC. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting privat](#).

Bekerja dengan zona yang di-hosting publik

Zona yang di-hosting publik adalah kontainer yang berisi informasi tentang cara merutekan lalu lintas di internet untuk domain tertentu, seperti `example.com`, dan subdomainnya (`acme.example.com`, `zenith.example.com`). Anda mendapatkan zona yang di-hosting publik dengan salah satu dari dua cara berikut:

- Ketika Anda mendaftarkan domain dengan Amazon Route 53, kami membuat zona yang di-hosting secara otomatis untuk Anda.
- Ketika mentransfer layanan DNS untuk domain yang ada ke Route 53, Anda memulai dengan membuat zona yang di-hosting untuk domain. Untuk informasi selengkapnya, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Di kedua kasus, kemudian Anda membuat catatan di zona yang di-hosting untuk menentukan cara merutekan lalu lintas bagi domain dan subdomain. Misalnya, Anda dapat membuat catatan untuk merutekan lalu lintas `www.example.com` ke CloudFront distribusi atau ke server web di pusat data Anda. Untuk informasi lebih lanjut tentang catatan, lihat [Bekerja dengan catatan](#).

Topik ini menjelaskan cara menggunakan konsol Amazon Route 53 untuk membuat, mencantumkan, dan menghapus zona yang di-hosting publik.

Note

Anda juga dapat menggunakan zona host pribadi Route 53 untuk merutekan lalu lintas dalam satu atau lebih VPCs yang Anda buat dengan layanan Amazon VPC. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting privat](#).

Topik

- [Pertimbangan saat bekerja dengan zona yang di-hosting publik](#)
- [Membuat zona yang di-hosting publik](#)
- [Mendapatkan server nama untuk zona yang di-hosting publik](#)

- [Mencantumkan zona yang di-hosting publik](#)
- [Melihat metrik kueri DNS untuk zona yang di-hosting publik](#)
- [Menghapus zona yang di-hosting publik](#)
- [Memeriksa respons DNS dari Route 53](#)
- [Mengonfigurasi server nama label putih](#)
- [Catatan NS dan SOA yang dibuat Amazon Route 53 untuk zona yang di-hosting publik](#)
- [Mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik](#)

Pertimbangan saat bekerja dengan zona yang di-hosting publik

Perhatikan pertimbangan berikut saat bekerja dengan zona yang di-hosting publik:

Catatan NS dan SOA

Ketika Anda membuat zona yang di-hosting, Amazon Route 53 secara otomatis membuat catatan server nama (NS) dan catatan start of authority (SOA) untuk zona. Catatan NS mengidentifikasi empat server nama yang Anda berikan ke registrar atau layanan DNS sehingga kueri DNS dirutekan ke server nama Route 53. Untuk informasi lebih lanjut tentang catatan NS dan SOA, lihat [Catatan NS dan SOA yang dibuat Amazon Route 53 untuk zona yang di-hosting publik](#).

Beberapa zona yang di-hosting dengan nama yang sama

Anda dapat membuat lebih dari satu zona yang di-hosting dengan nama yang sama dan menambahkan catatan yang berbeda ke setiap zona yang di-hosting. Route 53 menetapkan empat server nama untuk setiap zona yang di-hosting, dan server nama berbeda untuk setiap zona. Saat Anda memperbarui catatan server nama registrar, perhatikan untuk menggunakan server nama Route 53 untuk zona yang di-hosting yang benar—zona yang berisi catatan yang akan digunakan Route 53 saat merespons kueri untuk domain Anda. Route 53 tidak pernah mengembalikan nilai untuk catatan di zona yang di-hosting lain dengan nama yang sama.

Set delegasi yang dapat digunakan kembali

Secara default, Route 53 menetapkan satu set empat nama server yang unik (dikenal secara kolektif sebagai set delegasi) untuk setiap zona yang di-hosting yang Anda buat. Jika ingin membuat sejumlah besar zona yang di-hosting, Anda dapat membuat set delegasi yang dapat digunakan kembali secara terprogram. (Set delegasi yang dapat digunakan kembali tidak tersedia di konsol Route 53.) Kemudian Anda dapat membuat zona yang di-hosting secara terprogram dan

menetapkan set delegasi yang dapat digunakan kembali yang sama—empat server nama yang sama—ke setiap zona yang di-hosting.

Set delegasi yang dapat digunakan kembali menyederhanakan migrasi layanan DNS ke Route 53 karena Anda dapat menginstruksikan registrar nama domain untuk menggunakan empat server nama yang sama untuk semua domain yang ingin diggunakan Route 53 sebagai layanan DNS. Untuk informasi selengkapnya, lihat [CreateReusableDelegationSet](#) di Referensi API Amazon Route 53.

Membuat zona yang di-hosting publik

Zona yang di-hosting publik adalah kontainer yang berisi informasi tentang cara merutekan lalu lintas di internet untuk domain tertentu, seperti `example.com`, dan subdomainnya (`acme.example.com`, `zenith.example.com`). Setelah membuat catatan di zona yang di-hosting, buat catatan yang menentukan cara merutekan lalu lintas untuk domain dan subdomain.

Pembatasan

Perhatikan batasan berikut untuk membuat zona yang dihosting dengan Route 53.

- Anda dapat membuat zona yang di-hosting hanya untuk domain yang izin administrasinya Anda miliki. Biasanya, ini berarti Anda memiliki domain, tetapi Anda mungkin mengembangkan aplikasi untuk pendaftar domain.
- Anda dapat membuat zona yang dihosting hanya untuk domain dan subdomain. Route 53 tidak mendukung hosting domain tingkat atas (TLD) seperti. `.com`

Cara membuat zona yang di-hosting publik menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Jika Anda baru mengenal Route 53, pilih Memulai di bawah Manajemen DNS.

Jika Anda sudah menggunakan Route 53, pilih Zona yang di-hosting pada panel navigasi.

3. Pilih Buat Zona yang di-hosting.
4. Di panel Buat Zona yang Di-hosting, masukkan nama domain yang lalu lintasnya ingin Anda rutekan. Secara opsional Anda juga dapat memasukkan komentar.

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

5. Untuk Jenis, terima nilai default Zona yang Di-hosting Publik.
6. Pilih Buat.
7. Membuat catatan yang menentukan cara merutekan lalu lintas untuk domain dan subdomain. Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).
8. Untuk menggunakan catatan di zona yang di-hosting baru untuk merutekan lalu lintas domain Anda, lihat topik yang berlaku:
 - Jika Anda membuat Route 53 sebagai layanan DNS untuk domain yang terdaftar dengan registrar domain lain, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).
 - Jika domain terdaftar dengan Route 53, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

Mendapatkan server nama untuk zona yang di-hosting publik

Anda mendapatkan server nama untuk zona yang di-hosting publik jika ingin mengubah layanan DNS untuk pendaftaran domain. Untuk informasi tentang cara mengubah layanan DNS, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Note

Beberapa registrar hanya mengizinkan Anda menentukan server nama menggunakan alamat IP; mereka tidak mengizinkan Anda menentukan nama domain yang memenuhi syarat. Jika registrar memerlukan penggunaan alamat IP, Anda bisa mendapatkan alamat IP untuk server nama menggunakan utilitas penggalian (untuk Mac, Unix, atau Linux) atau utilitas nslookup (untuk Windows). Kami jarang mengubah alamat IP server nama; jika kami perlu mengubah alamat IP, kami akan memberitahu Anda terlebih dahulu.

Cara mendapatkan server nama untuk zona yang di-hosting menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Dalam panel navigasi, klik Zona yang di-hosting.

3. Pada halaman Zona yang di-hosting, pilih tombol radio (bukan nama) untuk zona yang di-hosting, lalu pilih Lihat detail.
4. Pada halaman detail untuk zona yang di-hosting, pilih Detail zona yang di-hosting.
5. Catat empat server yang tercantum untuk Server nama.

Mencantumkan zona yang di-hosting publik

Anda dapat menggunakan konsol Amazon Route 53 untuk mencantumkan semua zona yang dihosting yang Anda buat dengan AWS akun saat ini. Untuk informasi tentang cara mencantumkan zona yang dihosting menggunakan API Route 53, lihat [ListHostedZones](#) di Referensi API Amazon Route 53.

Untuk membuat daftar zona yang dihosting publik yang terkait dengan AWS akun menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting. Halaman ini menampilkan daftar zona yang dihosting yang terkait dengan AWS akun yang saat ini Anda masuki.
3. Untuk memfilter zona yang di-hosting, gunakan bilah pencarian yang terletak di bagian atas tabel.

Perilaku pencarian tergantung pada apakah zona yang di-hosting berisi hingga 2.000 catatan atau lebih dari 2.000 catatan:

Hingga 2.000 zona yang dihosting

- Untuk menampilkan catatan yang memiliki nilai tertentu, klik bilah pencarian, pilih properti di daftar dropdown, dan masukkan nilai. Anda juga dapat memasukkan nilai secara langsung di bilah pencarian dan tekan Enter. Misalnya, untuk menampilkan zona yang di-hosting dengan nama yang dimulai dengan **abc**, masukkan nilai tersebut di bilah pencarian dan tekan Enter.
- Untuk hanya menampilkan zona yang di-hosting dengan jenis zona yang di-hosting yang sama, pilih jenis dalam daftar dropdown, dan masukkan jenis.

Lebih dari 2.000 zona yang dihosting

- Anda dapat mencari properti berdasarkan nama domain yang tepat, semua properti, dan jenis.

- Cari menggunakan nama domain yang tepat untuk hasil pencarian yang lebih cepat.

Melihat metrik kueri DNS untuk zona yang di-hosting publik

Anda dapat melihat jumlah total kueri DNS yang direspons Route 53 untuk zona yang di-hosting publik tertentu atau kombinasi zona yang di-hosting publik. Metrik muncul CloudWatch, yang memungkinkan Anda melihat grafik, memilih periode waktu yang ingin Anda lihat, dan menyesuaikan metrik dengan berbagai cara lain. Anda juga dapat membuat alarm dan mengonfigurasi notifikasi, sehingga Anda diberi tahu jika jumlah kueri DNS dalam jangka waktu tertentu berada di atas atau di bawah tingkat yang ditentukan.

Note

Route 53 secara otomatis mengirimkan jumlah kueri DNS CloudWatch untuk semua zona yang dihosting publik, jadi Anda tidak perlu mengonfigurasi apa pun sebelum dapat melihat metrik kueri. Tidak ada biaya untuk metrik kueri DNS.

Manakah kueri DNS yang dihitung?

Metrik hanya berisi kueri yang diteruskan pemecah masalah DNS ke Route 53. Jika pemecah masalah DNS telah meng-cache respons untuk kueri (seperti alamat IP untuk penyeimbang beban bagi example.com), pemecah masalah akan terus mengembalikan respons yang di-cache tanpa meneruskan kueri ke Route 53 hingga TTL untuk catatan yang sesuai kedaluwarsa.

Tergantung pada jumlah kueri DNS yang dikirim untuk nama domain (example.com) atau nama subdomain (www.example.com), penyelesaian yang digunakan pengguna, dan TTL untuk catatan, metrik kueri DNS mungkin berisi informasi tentang satu kueri saja dari beberapa ribu permintaan yang dikirimkan ke penyelesaian DNS. Untuk informasi selengkapnya tentang cara kerja DNS, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Kapan metrik kueri untuk zona yang dihosting mulai muncul? CloudWatch

Setelah Anda membuat zona yang dihosting, ada penundaan hingga beberapa jam sebelum zona yang dihosting dapat muncul CloudWatch. Selain itu, Anda harus mengirimkan kueri DNS untuk catatan di zona yang di-hosting agar ada data untuk ditampilkan.

Metrik hanya tersedia di US East (N. Virginia)

Untuk mendapatkan metrik di konsol, Anda harus memilih US East (N. Virginia) untuk Wilayah. Untuk mendapatkan metrik menggunakan AWS CLI, Anda harus membiarkan AWS Wilayah tidak ditentukan, atau `us-east-1` tentukan sebagai Wilayah. Metrik Route 53 tidak tersedia jika Anda memilih Wilayah lain.

CloudWatch metrik dan dimensi untuk kueri DNS

Untuk informasi tentang CloudWatch metrik dan dimensi untuk kueri DNS, lihat [Memantau zona yang dihosting menggunakan Amazon CloudWatch](#) Untuk informasi tentang CloudWatch metrik, lihat [Menggunakan CloudWatch metrik Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Mendapatkan data yang lebih detail tentang kueri DNS

Untuk mendapatkan informasi lebih detail tentang setiap kueri DNS yang direspons Route 53, termasuk nilai berikut, Anda dapat menonfigurasi pencatatan kueri:

- Domain atau subdomain yang diminta
- Tanggal dan waktu permintaan
- Tipe catatan DNS (seperti A atau AAAA)
- Lokasi edge Route 53 yang merespons kueri DNS
- Kode respons DNS, seperti `NoError` atau `ServFail`

Untuk informasi selengkapnya, lihat [Pencatatan kueri DNS publik](#).

Cara mendapatkan metrik kueri DNS

Tak lama setelah Anda membuat zona yang dihosting, Amazon Route 53 mulai mengirim metrik dan dimensi satu menit sekali. CloudWatch Anda dapat menggunakan prosedur berikut untuk melihat metrik di CloudWatch konsol atau melihatnya menggunakan AWS Command Line Interface (AWS CLI).

Topik

- [Melihat metrik kueri DNS untuk zona yang dihosting publik di konsol CloudWatch](#)
- [Mendapatkan metrik kueri DNS menggunakan AWS CLI](#)

Melihat metrik kueri DNS untuk zona yang dihosting publik di konsol CloudWatch

Untuk melihat metrik kueri DNS untuk zona yang dihosting publik di CloudWatch konsol, lakukan prosedur berikut.

Untuk melihat metrik kueri DNS untuk zona yang dihosting publik di konsol CloudWatch

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pada daftar AWS Wilayah di sudut kanan atas konsol, pilih US East (Virginia N.). Metrik Route 53 tidak tersedia jika Anda memilih AWS Wilayah lain.
4. Pada tab Semua metrik, pilih Route 53.
5. Pilih Metrik Zona yang Di-hosting.
6. Pilih kotak centang untuk satu atau beberapa zona yang dihosting yang memiliki nama metrik DNSQueries.
7. Pada tab Metrik grafis, ubah nilai yang ada untuk melihat metrik dalam format yang Anda inginkan.

Untuk Statistik, pilih Jumlah atau SampleCount; statistik ini keduanya menampilkan nilai yang sama.

Mendapatkan metrik kueri DNS menggunakan AWS CLI

Untuk mendapatkan metrik kueri DNS menggunakan AWS CLI, Anda menggunakan perintah. [get-metric-data](#) Perhatikan hal-hal berikut:

- Anda menentukan sebagian besar nilai untuk perintah dalam file JSON terpisah. Untuk informasi selengkapnya, lihat [get-metric-data](#).
- Perintah mengembalikan satu nilai bagi setiap interval yang Anda tentukan untuk `Period` dalam file JSON. `Period` dalam hitungan detik, jadi jika Anda menentukan jangka waktu lima menit dan menentukan 60 untuk `Period`, Anda mendapatkan nilai lima. Jika Anda menentukan jangka waktu lima menit dan menentukan 300 untuk `Period`, Anda mendapatkan nilai satu.
- Dalam file JSON, Anda dapat menentukan nilai apapun untuk `Id`.
- Biarkan AWS Wilayah tidak ditentukan, atau tentukan `us-east-1` sebagai Wilayah. Metrik Route 53 tidak tersedia jika Anda memilih Wilayah lain. Untuk informasi selengkapnya, lihat [Mengonfigurasi AWS CLI](#) di Panduan Pengguna AWS Command Line Interface .

Berikut adalah AWS CLI perintah yang Anda gunakan untuk mendapatkan metrik kueri DNS untuk periode waktu lima menit antara 4:01 dan 4:07 pada 1 Mei 2019. Parameter `metric-data-queries` merujuk file JSON sampel yang mengikuti perintah.

```
aws cloudwatch get-metric-data --metric-data-queries file:///./metric.json --start-time 2019-05-01T04:01:00Z --end-time 2019-05-01T04:07:00Z
```

Berikut adalah file JSON sampel:

```
[
  {
    "Id": "my_dns_queries_id",
    "MetricStat": {
      "Metric": {
        "Namespace": "AWS/Route53",
        "MetricName": "DNSQueries",
        "Dimensions": [
          {
            "Name": "HostedZoneId",
            "Value": "Z1D633PJN98FT9"
          }
        ]
      },
      "Period": 60,
      "Stat": "Sum"
    },
    "ReturnData": true
  }
]
```

Inilah output dari perintah ini. Perhatikan hal-hal berikut:

- Waktu mulai dan waktu selesai dalam perintah mencakup periode waktu tujuh menit, 2019-05-01T04:01:00Z hingga 2019-05-01T04:07:00Z.
- Hanya ada enam nilai kembali. Tidak ada nilai untuk 2019-05-01T04:05:00Z karena tidak ada kueri DNS selama menit tersebut.
- Nilai `Period` yang ditentukan dalam file JSON adalah 60 (detik), sehingga nilai dilaporkan dalam interval satu menit.

```
{
```

```
"MetricDataResults": [
  {
    "Id": "my_dns_queries_id",
    "StatusCode": "Complete",
    "Label": "DNSQueries",
    "Values": [
      101.0,
      115.0,
      103.0,
      127.0,
      111.0,
      120.0
    ],
    "Timestamps": [
      "2019-05-01T04:07:00Z",
      "2019-05-01T04:06:00Z",
      "2019-05-01T04:04:00Z",
      "2019-05-01T04:03:00Z",
      "2019-05-01T04:02:00Z",
      "2019-05-01T04:01:00Z"
    ]
  }
]
```

Menghapus zona yang di-hosting publik

Bagian ini menjelaskan cara menghapus zona yang di-hosting publik menggunakan konsol Amazon Route 53.

Anda dapat menghapus zona yang di-hosting hanya jika tidak ada catatan selain catatan SOA dan NS default. Jika zona yang di-hosting berisi catatan lain, Anda harus menghapusnya sebelum Anda dapat menghapus zona yang di-hosting. Hal ini mencegah Anda agar tidak menghapus zona yang di-hosting yang masih berisi catatan secara tidak sengaja.

Topik

- [Mencegah lalu lintas agar tidak dirutekan ke domain](#)
- [Menghapus zona yang di-hosting publik yang dibuat oleh layanan lain](#)
- [Menggunakan konsol Route 53 untuk menghapus zona yang di-hosting publik](#)

Mencegah lalu lintas agar tidak dirutekan ke domain

Jika ingin tetap melakukan pendaftaran domain namun ingin menghentikan perutean lalu lintas internet ke situs web atau aplikasi web, sebaiknya hapus catatan di zona yang di-hosting alih-alih menghapus zona yang di-hosting.

Important

Jika zona yang di-hosting dihapus, Anda tidak dapat membatalkan penghapusannya. Anda harus membuat zona yang di-hosting baru dan memperbarui server nama untuk pendaftaran domain, yang dapat membutuhkan hingga 48 jam untuk diterapkan. Selain itu, jika Anda menghapus zona yang di-hosting, seseorang dapat membajak domain dan merutekan lalu lintas ke sumber daya mereka sendiri menggunakan nama domain Anda.

Jika Anda mendelegasikan tanggung jawab untuk subdomain ke zona yang di-hosting dan ingin menghapus zona yang di-hosting anak, Anda juga harus memperbarui zona yang di-hosting induk dengan menghapus catatan NS dengan nama yang sama sebagai zona yang di-hosting anak. Misalnya, jika ingin menghapus zona yang di-hosting `acme.example.com`, Anda juga harus menghapus catatan NS `acme.example.com` dalam zona yang di-hosting `example.com`. Kami merekomendasikan agar Anda menghapus catatan NS terlebih dahulu, dan menunggu durasi TTL pada catatan NS sebelum Anda menghapus zona yang di-hosting anak. Hal ini memastikan agar orang lain tidak dapat membajak zona yang di-hosting anak selama penyelesaian DNS masih memiliki server nama untuk zona yang di-hosting anak yang di-cache.

Jika ingin menghindari biaya bulanan zona yang di-hosting, Anda dapat mentransfer layanan DNS untuk domain ke layanan DNS gratis. Ketika mentransfer layanan DNS, Anda harus memperbarui server nama untuk pendaftaran domain. Jika domain terdaftar dengan Route 53, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#) untuk informasi tentang cara mengganti server nama Route 53 dengan server nama untuk layanan DNS baru. Jika domain terdaftar dengan registrar lain, gunakan metode yang disediakan oleh registrar untuk memperbarui server nama bagi pendaftaran domain. Untuk informasi lebih lanjut, lakukan pencarian "layanan DNS gratis" di internet.

Menghapus zona yang di-hosting publik yang dibuat oleh layanan lain

Jika zona yang di-hosting dibuat oleh layanan lain, Anda tidak dapat menghapusnya menggunakan konsol Route 53. Sebagai gantinya, Anda perlu menggunakan proses yang berlaku untuk layanan lainnya:

- **AWS Cloud Map**— Untuk menghapus zona host yang AWS Cloud Map dibuat saat Anda membuat namespace DNS publik, hapus namespace. AWS Cloud Map menghapus zona yang dihosting secara otomatis. Untuk informasi selengkapnya, lihat [Menghapus namespace](#) di Panduan Developer AWS Cloud Map .
- **Penemuan Layanan Amazon Elastic Container Service (Amazon ECS)** – Untuk menghapus zona yang di-hosting publik yang dibuat Amazon ECS ketika Anda membuat layanan menggunakan penemuan layanan, hapus layanan Amazon ECS yang menggunakan namespace, dan hapus namespace. Untuk informasi lebih lanjut, lihat [Menghapus layanan](#) dalam Panduan Developer Amazon Elastic Container Service.

Menggunakan konsol Route 53 untuk menghapus zona yang di-hosting publik

Untuk menggunakan konsol Route 53 guna menghapus zona yang di-hosting publik, lakukan prosedur berikut.

Cara menghapus zona yang di-hosting publik menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang dihosting, dan pilih tautan yang disorot untuk zona yang dihosting yang ingin Anda hapus.
3. Mengonfirmasi bahwa zona yang di-hosting yang ingin Anda hapus hanya berisi catatan NS dan SOA. Jika berisi catatan tambahan, hapuslah. Anda juga harus menonaktifkan penandatanganan DNSSEC:

Note

Jika Anda mencoba menghapus zona yang dihosting tanpa menyelesaikan persyaratan ini, Route 53 akan menampilkan kesalahan:

- Jika penandatanganan DNSSEC diaktifkan: Zona host yang ditentukan berisi Kunci Penandatanganan Kunci DNSSEC sehingga tidak dapat dihapus

- Jika kumpulan catatan sumber daya lain ada (selain catatan SOA dan NS default): Zona host yang ditentukan berisi kumpulan catatan sumber daya yang tidak diperlukan sehingga tidak dapat dihapus

- Pada halaman detail zona yang dihosting, dalam daftar Catatan, jika daftar catatan menyertakan catatan apa pun yang nilai kolom Type adalah sesuatu selain NS atau SOA, pilih baris, dan pilih Hapus.

Untuk memilih beberapa catatan berturut-turut, pilih baris pertama, tekan dan tahan tombol Shift, dan pilih baris terakhir. Untuk memilih beberapa catatan tidak berturut-turut, pilih baris pertama, tekan dan tahan tombol Ctrl, dan pilih baris yang tersisa.

 Note

Jika Anda membuat catatan NS untuk subdomain di zona yang di-hosting, hapus juga catatan tersebut.

4. Kembali ke halaman Zona yang dihosting, dan pilih baris untuk zona yang dihosting yang ingin Anda hapus.
5. Pilih Hapus.
6. Ketik kunci konfirmasi dan pilih Hapus.
7. Jika Anda ingin membuat domain tidak tersedia di internet, kami sarankan Anda mentransfer layanan DNS ke layanan DNS gratis lalu hapus zona yang di-hosting Route 53. Hal ini mencegah kueri DNS agar tidak salah dirutekan di masa mendatang.

Jika domain terdaftar dengan Route 53, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#) untuk informasi tentang cara mengganti server nama Route 53 dengan server nama untuk layanan DNS baru. Jika domain yang terdaftar dengan registrar lain, gunakan metode yang disediakan oleh registrar untuk mengubah server nama domain.

 Note

Jika menghapus zona yang di-hosting untuk subdomain (acme.example.com), Anda tidak perlu mengubah server nama untuk domain tersebut (example.com).

Memeriksa respons DNS dari Route 53

Jika membuat zona yang di-hosting Amazon Route 53 untuk domain, Anda dapat menggunakan alat pemeriksa DNS di konsol untuk melihat cara Route 53 merespons kueri DNS jika Anda mengonfigurasi domain untuk menggunakan Route 53 sebagai layanan DNS. Untuk catatan geolokasi, geoproximity, dan latensi, Anda juga dapat mensimulasikan kueri dari alamat IP and/or klien DNS resolver tertentu untuk mengetahui respons apa yang akan dikembalikan Route 53.

Important

Alat tidak mengirimkan kueri ke Domain Name System, alat hanya merespons berdasarkan pengaturan dalam catatan di zona yang di-hosting. Alat mengembalikan informasi yang sama terlepas dari apakah zona yang di-hosting saat ini sedang digunakan untuk merutekan lalu lintas untuk domain.

Alat pemeriksa DNS hanya berfungsi untuk zona yang di-hosting publik.

Note

Alat pemeriksaan DNS mengembalikan informasi yang mirip dengan apa yang Anda harapkan dari bagian jawaban `dig` perintah. Oleh karena itu, jika Anda meminta server nama subdomain yang mengarah ke server nama induk, itu tidak akan dikembalikan.

Topik

- [Menggunakan alat pemeriksa untuk melihat cara Amazon Route 53 merespons kueri DNS](#)
- [Menggunakan alat pemeriksa untuk mensimulasikan kueri dari alamat IP tertentu \(hanya catatan geolokasi dan latensi\)](#)

Menggunakan alat pemeriksa untuk melihat cara Amazon Route 53 merespons kueri DNS

Anda dapat menggunakan alat untuk melihat respons yang dikembalikan Amazon Route 53 dalam menanggapi kueri DNS untuk catatan.

Cara menggunakan alat pemeriksa untuk melihat cara Amazon Route 53 merespons kueri DNS

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang Di-hosting.
3. Pada halaman Zona yang Di-hosting, pilih nama zona yang di-hosting. Konsol menampilkan daftar catatan untuk zona yang di-hosting tersebut.
4. Untuk langsung membuka halaman Periksa respons dari Route 53, pilih Catatan pengujian.
5. Tentukan nilai-nilai berikut ini:
 - Nama catatan, tidak termasuk nama zona yang di-hosting. Sebagai contoh, untuk memeriksa `www.example.com`, masukkan `www`. Untuk memeriksa `example.com`, kosongkan bidang Nama catatan.
 - Jenis catatan yang ingin Anda periksa, seperti A atau CNAME.
6. Pilih Dapatkan Respons.
7. Bagian Respons yang dikembalikan oleh Route 53 mencakup nilai-nilai berikut:

Kode respons DNS

Kode yang menunjukkan apakah kueri tersebut valid atau tidak. Kode respons yang paling umum adalah NOERROR, yang berarti bahwa kueri tersebut valid. Jika respons tidak valid, Route 53 mengembalikan kode respons yang menjelaskan alasannya. Untuk daftar kode respons yang mungkin muncul, lihat [DNS RCODE](#) di situs web IANA.

Protokol

Protokol yang digunakan Amazon Route 53 untuk merespons kueri, baik UDP atau TCP.

Respons yang dikembalikan oleh Route 53

Nilai yang akan dikembalikan Route 53 ke aplikasi web. Nilainya adalah salah satu dari berikut ini:

- Untuk catatan non-alias, respons berisi nilai atau nilai-nilai dalam catatan.
- Untuk beberapa catatan dengan nama dan jenis yang sama, yang mencakup tertimbang, latensi, geolokasi, dan failover, respons berisi nilai dari catatan yang sesuai, berdasarkan permintaan.

- Untuk catatan alias yang merujuk ke AWS sumber daya selain catatan lain, respons berisi alamat IP atau nama domain untuk AWS sumber daya, tergantung pada jenis sumber daya.
- Untuk catatan alias yang merujuk ke catatan lain, respons berisi nilai atau nilai-nilai dari catatan yang dirujuk.

Menggunakan alat pemeriksa untuk mensimulasikan kueri dari alamat IP tertentu (hanya catatan geolokasi dan latensi)

Jika telah membuat catatan latensi atau geolokasi, Anda dapat menggunakan alat pemeriksa untuk mensimulasikan kueri dari alamat IP untuk penyelesai DNS dan klien.

Untuk menggunakan alat pemeriksa guna mensimulasikan kueri dari alamat IP yang ditentukan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang Di-hosting.
3. Pada halaman Zona yang Di-hosting, pilih nama zona yang di-hosting. Konsol menampilkan daftar catatan untuk zona yang di-hosting tersebut.
4. Untuk langsung membuka halaman Periksa respons dari Route 53, pilih Set catatan pengujian.

Untuk membuka halaman Periksa respons dari Route 53 untuk catatan tertentu, pilih kotak centang untuk catatan tersebut dan pilih Set catatan pengujian.

5. Jika Anda memilih Set catatan pengujian tanpa memilih catatan terlebih dahulu, tentukan nilai-nilai berikut:
 - Nama catatan, tidak termasuk nama zona yang di-hosting. Sebagai contoh, untuk memeriksa `www.example.com`, masukkan `www`. Untuk memeriksa `example.com`, kosongkan bidang Nama catatan.
 - Jenis catatan yang ingin Anda periksa, seperti A atau CNAME.
6. Tentukan nilai-nilai yang berlaku:

Alamat IP penyelesai

Tentukan IPv6 alamat IPv4 atau untuk mensimulasikan lokasi resolver DNS yang digunakan klien untuk membuat permintaan. Hal ini berguna untuk menguji catatan latensi dan

geolokasi. Jika Anda menghilangkan nilai ini, alat ini menggunakan alamat IP dari penyelesai DNS di Wilayah AWS AS Timur (Virginia N.) (us-east-1).

IP subnet klien EDNS0

Jika penyelesai mendukung EDNS0, masukkan IP subnet klien untuk alamat IP di lokasi geografis yang berlaku, misalnya, 192.0.2.0 atau 2001:db8:85a3::8a2e:370:7334.

Subnet mask

Jika Anda menentukan alamat IP untuk IP subnet klien EDNS0, Anda dapat menentukan jumlah bit alamat IP yang ingin disertakan alat pemeriksa ke dalam kueri DNS. Misalnya, jika Anda menentukan 192.0.2.44 untuk IP subnet klien EDNS0 dan 24 untuk Subnet mask, alat pemeriksa akan menyimulasikan kueri dari 192.0.2.0/24. Nilai default adalah 24 bit untuk IPv4 alamat dan 64 bit untuk IPv6 alamat.

7. Pilih Dapatkan Respons.
8. Bagian Respons yang dikembalikan oleh Route 53 mencakup nilai-nilai berikut:

Kueri DNS dikirimkan ke Route 53

Kueri, dalam [Format BIND](#), yang dikirimkan alat pemeriksa ke Route 53. Ini adalah format yang sama seperti yang digunakan aplikasi web untuk mengirim kueri. Tiga nilai biasanya berupa nama catatan, IN (untuk internet), dan jenis catatan.

Kode respons DNS

Kode yang menunjukkan apakah kueri tersebut valid atau tidak. Kode respons yang paling umum adalah NOERROR, yang berarti bahwa kueri tersebut valid. Jika respons tidak valid, Route 53 mengembalikan kode respons yang menjelaskan alasannya. Untuk daftar kode respons yang mungkin muncul, lihat [DNS RCODE](#) di situs web IANA.

Protokol

Protokol yang digunakan Amazon Route 53 untuk merespons kueri, baik UDP atau TCP.

Respons yang dikembalikan oleh Route 53

Nilai yang akan dikembalikan Route 53 ke aplikasi web. Nilainya adalah salah satu dari berikut ini:

- Untuk catatan non-alias, respons berisi nilai atau nilai-nilai dalam catatan.

- Untuk beberapa catatan dengan nama dan jenis yang sama, yang mencakup tertimbang, latensi, geolokasi, dan failover, respons berisi nilai dari catatan yang sesuai, berdasarkan permintaan.
- Untuk catatan alias yang merujuk ke AWS sumber daya selain catatan lain, respons berisi alamat IP atau nama domain untuk AWS sumber daya, tergantung pada jenis sumber daya.
- Untuk catatan alias yang merujuk ke catatan lain, respons berisi nilai atau nilai-nilai dari catatan yang dirujuk.

Mengonfigurasi server nama label putih

Setiap zona yang di-hosting Amazon Route 53 dikaitkan dengan empat server nama, dikenal secara kolektif sebagai set delegasi. Secara default, server nama memiliki nama seperti ns-2048.awsdns-64.com. Jika Anda ingin nama domain server agar sama dengan nama domain zona yang di-hosting, misalnya ns1.example.com, Anda dapat mengonfigurasi server nama label putih, juga dikenal sebagai server nama vanity atau server nama privat.

Langkah-langkah berikut menjelaskan cara mengonfigurasi satu set server nama label putih sejumlah empat buah yang dapat Anda gunakan kembali untuk beberapa domain. Misalnya, anggap Anda memiliki domain example.com, example.org, dan example.net. Dengan langkah-langkah ini, Anda dapat mengonfigurasi server nama label putih untuk example.com lalu menggunakannya kembali untuk example.org dan example.net.

Topik

- [Langkah 1: Membuat set delegasi Route 53 yang dapat digunakan kembali](#)
- [Langkah 2: Membuat atau membuat ulang zona yang di-hosting Amazon Route 53, dan mengubah TTL untuk catatan NS dan SOA](#)
- [Langkah 3: Membuat ulang catatan untuk zona yang di-hosting](#)
- [Langkah 4: Mendapatkan alamat IP](#)
- [Langkah 5: Membuat catatan untuk server nama label putih](#)
- [Langkah 6: Memperbarui catatan NS dan SOA](#)
- [Langkah 7: Membuat glue record dan mengubah server nama registrar](#)
- [Langkah 8: Memantau lalu lintas untuk situs web atau aplikasi](#)
- [Langkah 9: Ubah TTLs kembali ke nilai aslinya](#)
- [Langkah 10: \(Opsional\) Menghubungi layanan DNS rekursif](#)

Langkah 1: Membuat set delegasi Route 53 yang dapat digunakan kembali

Server nama label putih dikaitkan dengan set delegasi Route 53 yang dapat digunakan kembali. Anda dapat menggunakan server nama label putih untuk zona yang dihosting hanya jika zona yang dihosting dan kumpulan delegasi yang dapat digunakan kembali dibuat oleh akun yang sama. AWS

Untuk membuat kumpulan delegasi yang dapat digunakan kembali, Anda dapat menggunakan API Route 53, AWS CLI, atau salah satunya. AWS SDKs Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Route 53 API - Lihat [CreateReusableDelegationSet](#) di Referensi API Amazon Route 53
- AWS CLI - Lihat [create-reusable-delegation-set](#) di Referensi Perintah AWS CLI
- AWS SDKs Lihat dokumentasi SDK yang berlaku di halaman [AWS Dokumentasi](#)

Langkah 2: Membuat atau membuat ulang zona yang di-hosting Amazon Route 53, dan mengubah TTL untuk catatan NS dan SOA

Buat atau buat ulang zona yang di-hosting Amazon Route 53:

- Jika saat ini Anda tidak menggunakan Route 53 sebagai layanan DNS untuk domain yang ingin menggunakan server nama label putih – Membuat zona yang di-hosting dan menentukan set delegasi yang dapat digunakan kembali yang Anda buat di langkah sebelumnya dengan setiap zona yang di-hosting. Untuk informasi selengkapnya, lihat [CreateHostedZone](#) di Referensi API Amazon Route 53.
- Jika saat ini Anda menggunakan Route 53 sebagai layanan DNS untuk domain yang ingin menggunakan server nama label putih – Anda harus membuat ulang zona yang di-hosting yang ingin menggunakan server nama label putih, dan menentukan set delegasi yang dapat digunakan kembali yang Anda buat di langkah sebelumnya dengan setiap zona yang di-hosting.

Important

Anda tidak dapat mengubah server nama yang terkait dengan zona yang di-hosting yang sudah ada. Anda dapat mengaitkan set delegasi yang dapat digunakan kembali hanya dengan zona yang di-hosting ketika Anda membuat zona yang di-hosting.

Ketika Anda membuat zona yang di-hosting dan sebelum Anda mencoba mengakses sumber daya untuk domain yang sesuai, ubah nilai TTL berikut untuk setiap zona yang di-hosting:

- Ubah TTL catatan NS untuk zona yang di-hosting ke 60 detik atau kurang.
- Ubah TTL minimum catatan SOA untuk zona yang di-hosting ke 60 detik atau kurang. Ini adalah nilai terakhir dalam catatan SOA.

Jika Anda secara tidak sengaja memberikan alamat IP yang salah kepada registrar untuk server nama label putih, situs web Anda akan menjadi tidak tersedia dan tetap tidak tersedia selama TTL setelah Anda memperbaiki masalah. Dengan mengatur TTL yang rendah, Anda mengurangi jumlah waktu saat situs web tidak tersedia.

Untuk informasi selengkapnya tentang membuat zona yang dihosting dan menentukan set delegasi yang dapat digunakan kembali untuk server nama untuk zona yang dihosting, lihat [CreateHostedZone](#) di Referensi API Amazon Route 53.

Langkah 3: Membuat ulang catatan untuk zona yang di-hosting

Buat catatan di zona yang di-hosting yang Anda buat di Langkah 2:

- Jika Anda memigrasikan layanan DNS untuk domain Anda ke Amazon Route 53 — Anda mungkin dapat membuat catatan dengan mengimpor informasi tentang catatan yang ada. Untuk informasi selengkapnya, lihat [Membuat catatan dengan mengimpor file zona](#).
- Jika Anda mengganti zona yang di-hosting yang ada sehingga Anda dapat menggunakan server nama label putih – Di zona yang di-hosting baru, buat ulang catatan yang muncul di zona yang di-hosting saat ini. Route 53 tidak menyediakan metode mengekspor catatan dari zona yang di-hosting, tetapi beberapa vendor pihak ketiga yang menyediakannya. Anda kemudian dapat menggunakan fitur impor Route 53 untuk mengimpor catatan non-alias dengan kebijakan perutean yang sederhana. Tidak ada cara untuk mengekspor dan mengimpor ulang catatan alias atau catatan dengan kebijakan perutean yang tidak sederhana.

Untuk informasi tentang membuat rekaman menggunakan API Route 53, lihat [CreateHostedZone](#) di Referensi API Amazon Route 53. Untuk informasi tentang membuat catatan menggunakan konsol Route 53, lihat [Bekerja dengan catatan](#).

Langkah 4: Mendapatkan alamat IP

Dapatkan IPv4 dan IPv6 alamat server nama dalam set delegasi yang dapat digunakan kembali, dan isi tabel berikut.

Nama server nama di set delegasi yang dapat digunakan kembali (contoh: Ns-2048.awsdns-64.com)	IPv4 dan IPv6 alamat	Nama yang ingin Anda tetapkan ke server nama label putih (contoh: ns1.example.com)
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

Sebagai contoh, misalkan empat server nama untuk set delegasi yang dapat digunakan kembali adalah:

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Berikut adalah perintah Linux dan Windows yang akan Anda jalankan guna mendapatkan alamat IP yang pertama dari empat server nama:

perintah dig untuk Linux

```
% dig A ns-2048.awsdns-64.com +short
192.0.2.117
```

```
% dig AAAA ns-2048.awsdns-64.com +short
```

```
2001:db8:85a3::8a2e:370:7334
```

perintah nslookup untuk Windows

```
c:\> nslookup ns-2048.awsdns-64.com
Non-authoritative answer:
Name:      ns-2048.awsdns-64.com
Addresses: 2001:db8:85a3::8a2e:370:7334
           192.0.2.117
```

Langkah 5: Membuat catatan untuk server nama label putih

Di zona yang di-hosting dengan nama yang sama (seperti example.com) seperti nama domain server nama label putih (seperti ns1.example.com), buat delapan catatan:

- Satu catatan A untuk setiap server nama label putih
- Satu catatan AAAA untuk setiap server nama label putih

Important

Jika Anda menggunakan server nama label putih yang sama untuk dua atau lebih zona yang di-hosting, jangan lakukan langkah ini untuk zona yang di-hosting lainnya.

Untuk setiap catatan, tentukan nilai berikut. Lihat tabel yang Anda isi untuk langkah sebelumnya:

Kebijakan perutean

Tentukan Perutean sederhana.

Nama catatan

Nama yang ingin Anda tetapkan ke salah satu server nama label putih, misalnya ns1.example.com. Untuk prefiks (ns1 dalam contoh ini), Anda dapat menggunakan nilai yang valid dalam nama domain.

Nilai/Rutekan lalu lintas ke

IPv6 Alamat IPv4 atau salah satu server nama Route 53 di set delegasi yang dapat digunakan kembali.

 Important

Jika Anda menentukan alamat IP yang salah ketika membuat catatan untuk server nama label putih, situs web atau aplikasi web akan menjadi tidak tersedia di internet ketika Anda melakukan langkah-langkah berikutnya. Bahkan jika Anda segera memperbaiki alamat IP, situs web atau aplikasi web akan tetap tidak tersedia selama durasi TTL.

Tipe catatan

Tentukan A saat Anda membuat catatan untuk IPv4 alamat.

Tentukan AAAA saat Anda membuat catatan untuk alamat IPv6.

TTL (detik)

Nilai ini adalah jumlah waktu yang digunakan penyelesai DNS untuk meng-cache informasi dalam catatan ini sebelum meneruskan kueri DNS lain ke Route 53. Kami sarankan Anda menentukan nilai awal 60 detik atau kurang, sehingga Anda dapat memulihkan dengan cepat jika Anda secara tidak sengaja menentukan nilai yang salah dalam catatan ini.

Langkah 6: Memperbarui catatan NS dan SOA

Perbarui catatan SOA dan NS di zona yang di-hosting yang ingin menggunakan server nama label putih. Lakukan Langkah 6 hingga Langkah 8 untuk satu zona yang di-hosting dan domain yang sesuai secara bersamaan, lalu ulangi untuk zona yang di-hosting dan domain lainnya.

 Important

Mulai dengan zona yang di-hosting Amazon Route 53 dengan nama domain yang sama (seperti `example.com`) seperti server nama label putih (seperti `ns1.example.com`).

1. Memperbarui catatan SOA dengan mengganti nama server nama Route 53 dengan nama salah satu server nama label putih

Contoh

Mengganti nama server nama Route 53:

ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60

dengan nama salah satu server nama label putih Anda:

ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60

 Note

Anda mengubah nilai terakhir, waktu untuk tayang (TTL), di [Langkah 2: Membuat atau membuat ulang zona yang di-hosting Amazon Route 53, dan mengubah TTL untuk catatan NS dan SOA.](#)

Untuk informasi tentang memperbarui catatan menggunakan konsol Route 53, lihat [Mengedit catatan](#).

2. Dalam catatan NS, catat nama server nama untuk domain saat ini, sehingga Anda dapat kembali ke server nama ini jika diperlukan.
3. Perbarui catatan NS. Ganti nama server nama Route 53 dengan nama keempat server nama empat label putih Anda, misalnya, *ns1.example.com*, *ns2.example.com*, *ns3.example.com*, dan *ns4.example.com*.

Langkah 7: Membuat glue record dan mengubah server nama registrar

Gunakan metode yang disediakan oleh registrar untuk membuat glue record dan ubah server nama registrar:

1. Menambahkan glue record:
 - Jika Anda memperbarui domain dengan nama domain yang sama seperti server nama label putih – Buat empat glue record dengan nama dan alamat IP yang sesuai dengan nilai yang Anda dapatkan di langkah 4. Sertakan alamat IPv4 dan IPv6 alamat untuk server nama label putih dalam catatan lem yang sesuai, misalnya:

ns1.example.com – alamat IP = 192.0.2.117 dan 2001:db8:85a3::8a2e:370:7334

Registrar menggunakan berbagai terminologi untuk glue record. Anda mungkin juga melihat ini disebut sebagai mendaftarkan server nama baru atau yang serupa.

- Jika Anda memperbarui domain lain — Jika Route 53 adalah layanan DNS Anda, Anda harus terlebih dahulu menyelesaikan langkah di bullet sebelumnya dan membuat catatan lem yang cocok dengan nama domain. Kemudian lewati ke langkah 2 dalam prosedur ini.

2. Ubah server nama untuk domain ke nama server nama label putih Anda.

Jika Anda menggunakan Amazon Route 53 sebagai layanan DNS, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

Langkah 8: Memantau lalu lintas untuk situs web atau aplikasi

Pantau lalu lintas untuk situs web atau aplikasi dengan glue record yang Anda buat dan ubah server nama di Langkah 7:

- Jika lalu lintas berhenti – Gunakan metode yang disediakan oleh registrar guna mengembalikan server nama untuk domain ke server nama Route 53 sebelumnya. Ini adalah server nama yang Anda catat di langkah 6b. Kemudian tentukan apa yang salah.
- Jika lalu lintas tidak terpengaruh – Ulangi Langkah 6 hingga Langkah 8 untuk zona yang di-hosting yang tersisa dan ingin menggunakan server nama label putih yang sama.

Langkah 9: Ubah TTLs kembali ke nilai aslinya

Untuk semua zona yang di-hosting yang saat ini menggunakan server nama label putih, ubah nilai berikut:

- Ubah TTL catatan NS untuk zona yang di-hosting menjadi nilai yang lebih khas bagi catatan NS, misalnya 172.800 detik (dua hari).
- Ubah TTL minimum catatan SOA untuk zona yang di-hosting menjadi nilai yang lebih khas bagi catatan SOA, misalnya 900 detik. Ini adalah nilai terakhir dalam catatan SOA.

Langkah 10: (Opsional) Menghubungi layanan DNS rekursif

Opsional Jika Anda menggunakan perutean geolokasi Amazon Route 53, hubungi layanan DNS rekursif yang mendukung edns-client-subnet ekstensi EDNS0, dan beri mereka nama server nama label putih Anda. Hal ini memastikan bahwa layanan DNS akan terus merutekan kueri DNS ke lokasi Route 53 yang optimal berdasarkan perkiraan lokasi geografis tempat kueri berasal.

Catatan NS dan SOA yang dibuat Amazon Route 53 untuk zona yang di-hosting publik

Untuk setiap zona yang di-hosting publik yang Anda buat, Amazon Route 53 secara otomatis membuat catatan server nama (NS) dan catatan start of authority (SOA) untuk zona. Catatan ini tidak perlu sering diubah.

Topik

- [Catatan server nama \(NS\)](#)
- [Catatan start of authority \(SOA\)](#)

Catatan server nama (NS)

Amazon Route 53 secara otomatis membuat catatan server nama (NS) yang memiliki nama yang sama seperti zona yang di-hosting. Catatan ini mencantumkan empat server nama yang merupakan server nama otoritatif untuk zona yang di-hosting. Kecuali dalam situasi yang jarang terjadi, kami menyarankan agar Anda tidak menambahkan, mengubah, atau menghapus server nama dalam catatan ini.

Contoh berikut menampilkan format untuk nama server nama Route 53 (ini hanya contoh; jangan menggunakannya saat Anda memperbarui catatan server nama registrar):

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Untuk mendapatkan daftar server nama bagi zona yang di-hosting:

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Dalam panel navigasi, klik Zona yang di-hosting.
3. Pada halaman Zona yang di-hosting, pilih tombol radio (bukan nama) untuk zona yang di-hosting, lalu pilih Lihat detail.
4. Pada halaman detail untuk zona yang di-hosting, pilih Detail zona yang di-hosting.
5. Catat empat server yang tercantum untuk Server nama.

Untuk informasi tentang memigrasi layanan DNS dari penyedia layanan DNS lain ke Route 53, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Catatan start of authority (SOA)

Catatan start of authority (SOA) mengidentifikasi informasi DNS dasar tentang domain, misalnya:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

Catatan SOA mencakup elemen berikut:

- Server nama Route 53 yang membuat catatan SOA, misalnya, `ns-2048.awsdns-64.net`.
- Alamat email administrator. Simbol `@` diganti dengan tanda titik, misalnya, `hostmaster.example.com`. Nilai default adalah alamat email `amazon.com` yang tidak dipantau.
- Nomor seri yang secara opsional sapat Anda tambahkan setiap kali Anda memperbarui catatan di zona yang di-hosting. Route 53 tidak menambahkan nomor secara otomatis. (Nomor seri digunakan oleh layanan DNS yang mendukung DNS sekunder.) Dalam contoh ini, nilainya adalah `1`.
- Waktu penyegaran dalam hitungan detik yang merupakan waktu tunggu server DNS sekunder sebelum mengkueri catatan SOA server DNS primer untuk memeriksa perubahan. Dalam contoh ini, nilainya adalah `7200`.
- Interval percobaan ulang dalam hitungan detik yang merupakan waktu tunggu server sekunder sebelum mencoba kembali transfer zona yang gagal. Biasanya, waktu percobaan ulang kurang dari waktu penyegaran. Dalam contoh ini, nilainya adalah `900` (15 menit).
- Waktu dalam hitungan detik yang digunakan server sekunder untuk terus mencoba menyelesaikan transfer zona. Jika waktu ini berakhir sebelum transfer zona berhasil, server sekunder akan berhenti menjawab kueri karena menganggap data terlalu tua untuk dapat diandalkan. Dalam contoh ini, nilainya adalah `1209600` (dua minggu).
- Waktu untuk tayang (TTL) minimum. Nilai ini membantu menentukan durasi waktu yang harus di-cache penyelesai rekursif terkait respons dari Route 53:

NXDOMAIN

Tidak ada catatan dari jenis dengan nama yang ditentukan dalam kueri DNS, seperti `example.com`. Juga tidak ada catatan yang merupakan anak dari nama yang ditentukan dalam kueri DNS, seperti `zenith.example.com`.

NODATA

Ada setidaknya satu catatan dengan nama yang ditentukan dalam kueri DNS, tetapi tidak satu pun dari catatan memiliki jenis (seperti A) yang ditentukan dalam kueri DNS.

Ketika penyelesai DNS meng-cache respons NXDOMAIN atau NODATA respon, ini disebut sebagai caching negatif.

Durasi caching negatif lebih rendah dari nilai-nilai berikut:

- Nilai ini—TTL minimum dalam catatan SOA. Dalam contoh, nilainya adalah 86400 (satu hari).
- Nilai TTL untuk catatan SOA. Nilai default adalah 900 detik. Untuk informasi tentang perubahan nilai ini, lihat [Mengedit catatan](#).

Ketika Route 53 merespons kueri DNS dengan respons NXDOMAIN atau NODATA (respons negatif), Anda dikenakan tarif untuk kueri standar. (Lihat "Kueri" di [Harga Amazon Route 53](#). Jika Anda khawatir tentang biaya respons negatif, opsinya adalah mengubah TTL untuk catatan SOA, TTL minimum dalam catatan SOA (nilai ini), atau keduanya. Perhatikan bahwa meningkatkan ini TTLs, yang berlaku untuk respons negatif untuk seluruh zona yang dihosting, dapat memiliki efek positif dan negatif:

- Penyelesai DNS di internet meng-cache non-eksistensi catatan untuk jangka waktu yang lebih lama, mengurangi jumlah kueri yang diteruskan ke Route 53. Tindakan ini mengurangi biaya Route 53 untuk kueri DNS.
- Namun, jika Anda pernah keliru menghapus data yang valid dan kemudian membuat ulang data tersebut, penyelesai DNS akan meng-cache respons negatif (catatan ini tidak ada) untuk jangka waktu yang lebih lama. Ini memperpanjang jumlah waktu bagi pelanggan atau pengguna Anda tidak dapat mencapai sumber daya yang sesuai, seperti server web untuk `acme.example.com`.

Untuk menemukan catatan SOA Anda di Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama yang ditautkan dari domain yang ingin Anda lihat catatannya.
4. Pada bagian Catatan Anda dapat melihat semua catatan yang terdaftar dan Anda juga dapat memfilter catatan untuk menemukan nilai SOA Anda.

Mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik

Route 53 percepatan pemulihan untuk mengelola catatan DNS publik dirancang untuk mencapai 60 menit Recovery Time Objective (RTO) dalam hal tidak tersedianya layanan di Wilayah AS Timur (Virginia N.). Saat diaktifkan di zona yang dihosting publik Route 53, Anda akan dapat melanjutkan perubahan pada catatan DNS di zona yang dihosting publik dalam waktu sekitar 60 menit setelah AWS mendeteksi bahwa operasi di Wilayah AS Timur (Virginia N.) terganggu.

Important

Pemulihan yang dipercepat hanya tersedia untuk zona yang dihosting publik. Zona yang dihosting pribadi tidak didukung.

Note

Resolusi kueri DNS dari bidang data Route 53 terus bekerja secara normal selama gangguan layanan Regional. Lihat [Ketahanan di Rute 53](#) untuk pemahaman tentang bidang data versus operasi pesawat kontrol.

Topik

- [Bagaimana pemulihan yang dipercepat untuk catatan DNS publik bekerja](#)
- [Mengirimkan kembali perubahan DNS setelah failover](#)
- [Kegagalan Kembali ke Wilayah AS Timur \(Virginia N.\)](#)
- [Pertimbangan tambahan](#)
- [Cara mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik](#)

Bagaimana pemulihan yang dipercepat untuk catatan DNS publik bekerja

Saat pemulihan yang dipercepat diaktifkan, Route 53 akan menyimpan salinan zona host publik Anda di Wilayah Barat AS (Oregon). Jika layanan di Wilayah AS Timur (Virginia Utara) tidak tersedia untuk waktu yang lama, Route 53 akan mengeksekusi failover dalam waktu 60 menit, secara otomatis mengalihkan operasi pesawat kontrol untuk zona host publik yang diaktifkan pemulihan yang dipercepat ke Wilayah AS Barat (Oregon). Anda kemudian dapat terus membuat perubahan DNS secara terprogram melalui CLI, SDK, dan API. Perhatikan bahwa sekumpulan metode API terbatas

akan tersedia selama failover. Lihat bagian “Pertimbangan tambahan” untuk detail selengkapnya. Ketika wilayah pulih, Route 53 akan menjalankan prosedur failback, secara otomatis mengarahkan operasi pesawat kontrol kembali ke Wilayah AS Timur (Virginia N.).

Note

Sebelum terjadi kerusakan pada Wilayah AS Timur (Virginia N.), Anda harus terlebih dahulu mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik di zona host publik Anda. Ini dapat dilakukan melalui Konsol, CLI, SDK, atau API (lihat bagian berjudul Cara mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik pada halaman di bawah ini). Anda tidak dapat mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik setelah terjadi failover.

Mengirimkan kembali perubahan DNS setelah failover

Dalam kondisi normal, perubahan pada zona yang dihosting publik dengan pemulihan yang dipercepat diaktifkan akan diterima oleh Wilayah AS Timur (Virginia N.) dan kemudian akan berhasil direplikasi ke Wilayah Barat AS (Oregon). Namun, ketika gangguan layanan terjadi di Wilayah AS Timur (Virginia N.), beberapa perubahan dapat diterima oleh Wilayah AS Timur (Virginia N.), tetapi mungkin tidak direplikasi ke Wilayah Barat AS (Oregon). Perubahan dalam penerbangan ini disebut sebagai “perubahan terdampar”. Setelah failover selesai, Route 53 merekomendasikan agar Anda mengirimkan ulang perubahan yang terdampar sebelum melanjutkan alur kerja DNS Anda. Anda dapat mencapai ini baik dengan menggunakan API, atau dengan menggunakan AWS CloudFormation, yang dijelaskan di bawah ini.

Menggunakan API untuk melacak dan mengirimkan perubahan DNS

Jika Anda menggunakan API Route 53, AWS CLI, atau AWS SDKs untuk mengelola catatan DNS, maka Anda harus menggunakan [ChangeResourceRecordSets API](#) dan [GetChange API](#) untuk masing-masing mengirimkan dan melacak perubahan DNS.

Saat Anda menggunakan ChangeResourceRecordSets API untuk membuat perubahan DNS, Route 53 menampilkan pengenalan (ID) untuk perubahan yang Anda buat (lihat [ChangeInfo](#) detail objek respons perubahan). Anda dapat memberikan ID ini dalam permintaan berikutnya GetChange ke API dan mengamati status perubahan. Perubahan DNS dengan status INSYNC telah direplikasi ke Wilayah AS Barat (Oregon) dan disebarkan ke semua server DNS Route 53. Tidak ada tindakan lebih lanjut yang perlu Anda lakukan pada perubahan ini sebelum atau setelah failover. Namun,

selama penurunan nilai ke Wilayah AS Timur (Virginia N.), GetChange dapat kembali PENDING, menunjukkan perubahan Anda mungkin tidak direplikasi ke Wilayah AS Barat (Oregon). Jika itu masalahnya, ketika failover selesai, GetChange akan kembali NoSuchChange, menunjukkan bahwa Route 53 tidak dapat mereplikasi perubahan DNS ini. Oleh karena itu, setelah failover Anda dapat dengan aman mengabaikan perubahan DNS yang terdampar ini dan mengirimkannya kembali sebagai perubahan DNS baru. Anda akan tahu proses failover telah selesai ketika Route 53 memposting pesan ke Dasbor AWS Kesehatan.

Menggunakan AWS CloudFormation untuk melacak dan mengirimkan perubahan

AWS CloudFormation secara otomatis melacak status replikasi untuk perubahan DNS Anda menggunakan GetChange API, dan hanya menyelesaikan pembaruan setelah perubahan DNS dikonfirmasi sebagai INSYNC. Jika Anda menggunakan CloudFormation untuk mengelola catatan DNS dan Wilayah AS Timur (Virginia N.) menjadi tidak tersedia, maka tindakan yang Anda lakukan tidak CloudFormation akan berhasil diselesaikan selama periode tidak tersedianya. Namun, Anda cukup mencoba lagi tindakan yang sama CloudFormation untuk memungkinkan pengiriman ulang perubahan DNS, setelah proses failover Route 53 selesai.

Kegagalan Kembali ke Wilayah AS Timur (Virginia N.)

Route 53 akan gagal mengendalikan kembali operasi pesawat untuk zona host publik Anda ke Wilayah AS Timur (Virginia N.) setelah wilayah tersebut pulih. Selama failback, Anda tidak perlu mengirimkan ulang perubahan DNS Anda, karena tidak ada perubahan terdampar yang akan diperkenalkan selama proses ini.

Pertimbangan tambahan

Ada beberapa pertimbangan tambahan yang harus diperhatikan terkait dengan fitur pemulihan yang dipercepat:

1. Anda tidak akan dapat membuat zona host baru, menghapus zona host yang ada, mengaktifkan penandatanganan DNSSEC, atau menonaktifkan penandatanganan DNSSEC selama failover.
2. AWS PrivateLink koneksi tidak akan berfungsi setelah failover, tetapi akan berfungsi sekali lagi setelah gagal kembali ke Wilayah AS Timur (Virginia N.).
3. [CloudFront Paket flat-rate](#) tidak didukung saat ini.
4. Zona yang dihosting dengan pemulihan yang dipercepat diaktifkan tidak dapat dihapus. Anda harus menonaktifkan pemulihan yang dipercepat sebelum mencoba menghapus zona yang dihosting.

5. Selama failover, metode API berikut akan terus didukung untuk zona yang dihosting publik dengan pemulihan yang dipercepat diaktifkan. Namun, semua metode API Route 53 lainnya tidak akan berfungsi sampai kegagalan terjadi.

- `ChangeResourceRecordSets`
- `GetChange`
- `GetGeoLocation`
- `GetHostedZone`
- `GetHostedZoneCount`
- `GetHostedZoneLimit`
- `GetReusableDelegationSet`
- `GetReusableDelegationSetLimit`
- `ListGeoLocations`
- `ListHostedZones`
- `ListHostedZonesByName`
- `ListResourceRecordSets`
- `ListReusableDelegationSets`

Cara mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik

Anda dapat mengaktifkan pemulihan yang dipercepat untuk mengelola catatan DNS publik menggunakan konsol Route 53, API, CLI, atau SDK. Waktu yang diperlukan untuk mengaktifkan pemulihan yang dipercepat akan tergantung pada ukuran zona host publik Anda dan faktor lainnya. Anda harus merencanakan proses memungkinkan pemulihan yang dipercepat memakan waktu hingga beberapa jam. Anda dapat memeriksa status proses pemberdayaan di tab Pemulihan yang dipercepat di zona host publik Anda atau melalui `GetHostedZone` API. Saat proses selesai, akan ada periode waktu singkat yang berlangsung hingga beberapa menit di mana perubahan DNS tidak diterima. Setelah selesai, perubahan DNS dapat berjalan seperti biasa.

Untuk mengaktifkan dan menonaktifkan pemulihan yang dipercepat menggunakan konsol Route 53

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih zona yang dihosting publik yang ingin Anda aktifkan pemulihan yang dipercepat.
4. Di tab Accelerated Recovery, pilih Aktifkan.

5. Pilih Simpan perubahan.
6. Pantau status zona yang dihosting. Status menunjukkan Mengaktifkan pemulihan yang dipercepat selama penyiapan dan perubahan ke Diaktifkan saat selesai.

Anda dapat menonaktifkan pemulihan yang dipercepat menggunakan langkah-langkah yang sama di atas, tetapi memilih Nonaktifkan.

Contoh CLI untuk mengaktifkan

```
aws route53 update-hosted-zone-features --enable-accelerated-recovery --hosted-zone-id Z123456789
```

Contoh CLI untuk menonaktifkan

```
aws route53 update-hosted-zone-features --no-enable-accelerated-recovery --hosted-zone-id Z123456789
```

Bekerja dengan zona yang di-hosting privat

Zona yang dihosting pribadi adalah wadah yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 menanggapi kueri DNS untuk domain dan subdomainnya dalam satu atau lebih VPCs yang Anda buat dengan layanan Amazon VPC. Berikut adalah cara kerja zona yang di-hosting privat:

1. Anda membuat zona host pribadi, seperti example.com, dan menentukan VPC yang ingin Anda kaitkan dengan zona yang dihosting. Setelah Anda membuat zona yang dihosting, Anda dapat mengasosiasikan lebih banyak VPCs dengannya.
2. Anda membuat catatan di zona yang dihosting yang menentukan cara Route 53 merespons kueri DNS untuk domain dan subdomain Anda di dalam dan di antara Anda. VPCs Misalnya, Anda memiliki server database yang berjalan pada EC2 instance di VPC yang Anda kaitkan dengan zona host pribadi Anda. Anda membuat catatan A atau AAAA, seperti db.example.com, dan Anda menentukan alamat IP server basis data.

Untuk informasi lebih lanjut tentang catatan, lihat [Bekerja dengan catatan](#). Untuk informasi tentang persyaratan Amazon VPC untuk menggunakan zona yang di-hosting privat, lihat [Menggunakan zona yang di-hosting privat](#) dalam Panduan Pengguna Amazon VPC.

3. Ketika aplikasi mengirim kueri DNS untuk db.example.com, Route 53 mengembalikan alamat IP yang sesuai. Untuk mendapatkan jawaban dari zona host pribadi, Anda juga harus menjalankan

EC2 instance di salah satu yang terkait VPCs (atau memiliki titik akhir masuk dari pengaturan hibrida.) Jika Anda mencoba menanyakan zona host pribadi dari luar VPCs atau pengaturan hybrid Anda, kueri akan diselesaikan secara rekursif di internet.

4. Aplikasi ini menggunakan alamat IP yang didapat dari Route 53 untuk membuat koneksi dengan server basis data.

Saat Anda membuat zona host pribadi, server nama berikut akan digunakan:

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

Server nama ini digunakan karena protokol DNS mengharuskan setiap zona yang dihosting harus memiliki kumpulan catatan NS. Server nama ini dicadangkan dan tidak pernah digunakan oleh zona yang dihosting publik Route 53. Anda hanya dapat menanyakan zona tersebut melalui Resolver VPC di VPC yang telah dikaitkan dengan zona yang dihosting dengan menggunakan titik akhir masuk yang terhubung ke zona host pribadi yang ditentukan. VPCs

Sementara server nama terlihat di internet, VPC Resolver tidak terhubung ke alamat server nama. Selanjutnya, informasi zona yang dihosting pribadi tidak dikembalikan jika Anda langsung menanyakan server nama melalui internet. Sebagai gantinya, VPC Resolver mendeteksi bahwa kueri berada dalam namespace pribadi berdasarkan VPC ke asosiasi zona yang dihosting dan menggunakan konektivitas pribadi langsung untuk menjangkau server DNS pribadi.

Note

Anda dapat mengubah catatan NS yang ditetapkan di zona host pribadi jika Anda mau dan resolusi DNS pribadi akan tetap berfungsi. Kami tidak menyarankan melakukannya, tetapi jika Anda memilih untuk melakukannya, Anda harus menggunakan nama domain cadangan yang tidak digunakan oleh server DNS publik.

Jika ingin merutekan lalu lintas untuk domain di internet, Anda menggunakan zona yang di-hosting publik Route 53. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting publik](#).

Topik

- [Pertimbangan saat bekerja dengan zona yang di-hosting privat](#)
- [Membuat zona yang di-hosting privat](#)
- [Mencantumkan zona yang di-hosting privat](#)
- [Mengaitkan lebih banyak VPCs dengan zona yang dihosting pribadi](#)
- [Mengaitkan VPC Amazon dan zona host pribadi yang Anda buat dengan akun berbeda AWS](#)
- [Memutuskan hubungan VPCs dari zona yang dihosting pribadi](#)
- [Menghapus zona yang di-hosting privat](#)
- [Izin VPC](#)

Pertimbangan saat bekerja dengan zona yang di-hosting privat

Saat menggunakan zona yang di-hosting privat, perhatikan pertimbangan berikut.

- [Amazon VPC settings](#)
- [Route 53 health checks](#)
- [Supported routing policies for records in a private hosted zone](#)
- [Split-view DNS](#)
- [Public and private hosted zones that have overlapping namespaces](#)
- [Private hosted zones that have overlapping namespaces](#)
- [Private hosted zones and Route 53 VPC Resolver rules](#)
- [Delegating responsibility for a subdomain](#)
- [Custom DNS servers](#)
- [Required IAM permissions](#)

Pengaturan Amazon VPC

Untuk menggunakan zona yang di-hosting privat, Anda harus mengatur pengaturan Amazon VPC berikut ke `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Untuk informasi selengkapnya, lihat [Melihat dan memperbarui atribut DNS untuk VPC Anda](#) di Panduan Pengguna Amazon VPC.

Pemeriksaan kondisi Route 53

Di zona host pribadi, Anda dapat mengaitkan pemeriksaan kesehatan Route 53 hanya dengan catatan failover, jawaban multivalue, tertimbang, latensi, geolokasi, dan catatan geoproximity. Untuk informasi tentang mengaitkan pemeriksaan kondisi dengan catatan failover, lihat [Mengonfigurasi failover di zona yang di-hosting secara privat](#).

Kebijakan perutean yang didukung untuk catatan di zona yang di-hosting privat

Anda dapat menggunakan kebijakan perutean berikut ketika membuat catatan di zona yang di-hosting privat:

- [Perutean sederhana](#)
- [Perutean failover](#)
- [Perutean jawaban multinilai](#)
- [Perutean tertimbang](#)
- [Perutean berbasis latensi](#)
- [Perutean geolokasi](#)
- [Perutean geoproksimitas](#)

Membuat catatan di zona yang di-hosting privat menggunakan kebijakan perutean lainnya tidak didukung.

DNS split-view

Anda dapat menggunakan Route 53 untuk mengonfigurasi DNS split-view, juga dikenal sebagai DNS split-horizon. Di DNS split-view, Anda menggunakan nama domain yang sama (example.com) untuk penggunaan internal (accounting.example.com) dan penggunaan eksternal, seperti situs web publik (www.example.com). Anda mungkin juga ingin menggunakan nama subdomain yang sama secara internal dan eksternal, tetapi melayani konten yang berbeda atau memerlukan autentikasi yang berbeda untuk pengguna internal dan eksternal.

Untuk mengonfigurasi DNS split-view, lakukan langkah-langkah berikut:

1. Membuat zona yang di-hosting publik dan privat yang memiliki nama yang sama. (DNS split-view masih berfungsi jika Anda menggunakan layanan DNS lain untuk zona yang di-hosting publik.)
2. Kaitkan satu atau lebih Amazon VPCs dengan zona host pribadi. Route 53 VPC Resolver menggunakan zona host pribadi untuk merutekan kueri DNS dalam yang ditentukan. VPCs

3. Membuat catatan di setiap zona yang di-hosting. Catatan di zona yang dihosting publik mengontrol cara lalu lintas internet dirutekan, dan catatan di zona host pribadi mengontrol cara lalu lintas dirutekan di Amazon Anda. VPCs

Jika Anda perlu melakukan resolusi nama untuk VPC dan beban kerja lokal, Anda dapat menggunakan Route 53 VPC Resolver. Untuk informasi selengkapnya, lihat [Apa itu Route 53 VPC Resolver?](#).

Zona yang di-hosting publik dan privat dengan namespace yang tumpang tindih

Jika Anda memiliki zona host pribadi dan publik yang memiliki ruang nama yang tumpang tindih, seperti `example.com` dan `accounting.example.com`, VPC Resolver merutekan lalu lintas berdasarkan kecocokan paling spesifik. Saat pengguna masuk ke EC2 instance di VPC Amazon yang telah Anda kaitkan dengan zona host pribadi, inilah cara Route 53 VPC Resolver menangani kueri DNS:

1. VPC Resolver mengevaluasi apakah nama zona host pribadi cocok dengan nama domain dalam permintaan, seperti `accounting.example.com`. Kecocokan ditentukan sebagai berikut:
 - Kecocokan identik
 - Nama zona yang di-hosting privat adalah induk dari nama domain dalam permintaan. Misalnya, nama domain dalam permintaan adalah sebagai berikut:

`seattle.accounting.example.com`

Zona yang di-hosting berikut cocok karena mereka induk dari `seattle.accounting.example.com`:

- `accounting.example.com`
- `example.com`

Jika tidak ada zona host pribadi yang cocok, maka VPC Resolver meneruskan permintaan ke resolver DNS publik, dan permintaan Anda diselesaikan sebagai kueri DNS biasa.

2. Jika ada nama zona yang di-hosting privat yang cocok dengan nama domain dalam permintaan, zona yang di-hosting akan mencari catatan yang cocok dengan nama domain dan jenis DNS dalam permintaan, seperti catatan A untuk `accounting.example.com`.

Note

Jika ada zona host pribadi yang cocok tetapi tidak ada catatan yang cocok dengan nama domain dan mengetik permintaan, VPC Resolver tidak meneruskan permintaan

ke resolver DNS publik. Alih-alih, NXDOMAIN (domain tidak ada) dikembalikan ke klien.

Zona yang di-hosting privat dengan namespace yang tumpang tindih

Jika Anda memiliki dua atau lebih zona host pribadi yang memiliki ruang nama yang tumpang tindih, seperti `example.com` dan `accounting.example.com`, VPC Resolver merutekan lalu lintas berdasarkan kecocokan paling spesifik.

Note

Jika Anda memiliki zona host pribadi (`example.com`) dan aturan Resolver VPC Route 53 yang merutekan lalu lintas ke jaringan Anda untuk nama domain yang sama, aturan Resolver VPC akan diutamakan. Lihat [Private hosted zones and Route 53 VPC Resolver rules](#).

Saat pengguna masuk ke EC2 instance di VPC Amazon yang telah Anda kaitkan dengan semua zona yang dihosting pribadi, inilah cara VPC Resolver menangani kueri DNS:

1. VPC Resolver mengevaluasi apakah nama domain dalam permintaan, seperti `accounting.example.com`, cocok dengan nama salah satu zona yang dihosting pribadi.
2. Jika tidak ada zona host yang sama persis dengan nama domain dalam permintaan, VPC Resolver memeriksa zona yang dihosting yang memiliki nama yang merupakan induk dari nama domain dalam permintaan. Misalnya, nama domain dalam permintaan adalah sebagai berikut:

`seattle.accounting.example.com`

Zona yang di-hosting berikut cocok karena mereka induk dari

`seattle.accounting.example.com`:

- `accounting.example.com`
- `example.com`

VPC Resolver memilih `accounting.example.com` karena lebih spesifik daripada `example.com`

3. VPC Resolver mencari zona yang `accounting.example.com` dihosting untuk catatan yang cocok dengan nama domain dan jenis DNS dalam permintaan, seperti catatan A untuk `seattle.accounting.example.com`

Jika tidak ada catatan yang cocok dengan nama domain dan jenis permintaan, VPC Resolver mengembalikan NXDOMAIN (domain yang tidak ada) ke klien.

Zona yang dihosting pribadi dan aturan Route 53 VPC Resolver

Jika Anda memiliki zona host pribadi (example.com) dan aturan Resolver VPC yang merutekan lalu lintas ke jaringan Anda untuk nama domain yang sama, aturan Resolver VPC akan diutamakan.

Sebagai contoh, anggap Anda memiliki konfigurasi berikut:

- Anda memiliki zona yang di-hosting privat yang disebut example.com, dan mengaitkannya dengan VPC.
- Anda membuat aturan Resolver VPC Route 53 yang meneruskan lalu lintas contoh.com ke jaringan Anda, dan Anda mengaitkan aturan dengan VPC yang sama.

Dalam konfigurasi ini, aturan Resolver VPC lebih diutamakan daripada zona host pribadi. Kueri DNS diteruskan ke jaringan Anda, bukan diselesaikan berdasarkan catatan di zona yang di-hosting privat.

Mendelegasikan tanggung jawab untuk subdomain

Anda sekarang dapat membuat catatan NS di zona host pribadi untuk mendelegasikan tanggung jawab untuk subdomain. Untuk informasi selengkapnya, lihat [Tutorial aturan delegasi penyelesai](#).

Server DNS kustom

Jika Anda telah mengonfigurasi server DNS khusus pada EC2 instans Amazon di VPC Anda, Anda harus mengonfigurasi server DNS tersebut untuk merutekan kueri DNS pribadi Anda ke alamat IP server DNS yang disediakan Amazon untuk VPC Anda. Alamat IP ini adalah alamat IP di dasar rentang jaringan VPC "plus two". Misalnya, jika rentang CIDR untuk VPC adalah 10.0.0.0/16, alamat IP server DNS adalah 10.0.0.2.

Jika Anda ingin merutekan kueri DNS antara VPCs dan jaringan Anda, Anda dapat menggunakan VPC Resolver. Untuk informasi selengkapnya, lihat [Apa itu Route 53 VPC Resolver?](#).

Izin IAM yang diperlukan

Untuk membuat zona yang dihosting pribadi, Anda harus memberikan izin IAM untuk EC2 tindakan Amazon selain izin untuk tindakan Route 53. Untuk informasi selengkapnya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Rute 53](#) di Referensi Otorisasi Layanan.

Membuat zona yang di-hosting privat

Zona yang dihosting pribadi adalah wadah untuk catatan untuk domain yang Anda host di satu atau beberapa awan pribadi virtual Amazon (VPCs). Anda membuat zona yang dihosting untuk domain (seperti `example.com`), lalu Anda membuat catatan untuk memberi tahu Amazon Route 53 bagaimana Anda ingin lalu lintas dirutekan untuk domain tersebut di dalam dan di antara Anda. VPCs

Important

Ketika membuat zona yang di-hosting privat, Anda harus mengaitkan VPC dengan zona yang di-hosting, dan VPC yang Anda tentukan harus dibuat menggunakan akun yang sama yang Anda gunakan untuk membuat zona yang di-hosting. Setelah Anda membuat zona yang dihosting, Anda dapat mengaitkan tambahan VPCs dengannya, termasuk VPCs yang Anda buat dengan menggunakan AWS akun yang berbeda.

Untuk mengaitkan VPCs yang Anda buat dengan menggunakan satu akun dengan zona host pribadi yang Anda buat dengan menggunakan akun lain, Anda harus mengotorisasi asosiasi dan kemudian membuat asosiasi secara terprogram. Untuk informasi selengkapnya, lihat [Mengaitkan VPC Amazon dan zona host pribadi yang Anda buat dengan akun berbeda AWS](#).

Untuk informasi tentang membuat zona yang di-hosting privat menggunakan API Route 53, lihat [Referensi API Amazon Route 53](#).

Cara membuat zona yang di-hosting privat menggunakan konsol Route 53

1. Untuk setiap VPC yang ingin Anda kaitkan dengan zona yang di-hosting Route 53, ubah pengaturan VPC berikut ke `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Untuk informasi selengkapnya, lihat [Memperbarui DNS dukungan untuk VPC Anda](#) dalam Panduan Pengguna Amazon VPC.

2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Jika Anda baru mengenal Route 53, pilih **Memulai**

Jika Anda sudah menggunakan Route 53, pilih **Zona yang di-hosting** pada panel navigasi.

4. Pilih Buat Zona yang di-hosting.
5. Pada panel Buat zona yang di-hosting privat, masukkan nama domain dan, secara opsional, komentar.

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

6. Di daftar Jenis, pilih Zona yang di-hosting privat.
7. Di daftar ID VPC, pilih VPC yang ingin Anda kaitkan dengan zona yang di-hosting.

Note

Jika konsol menampilkan pesan berikut, Anda mencoba mengaitkan zona yang di-hosting yang menggunakan namespace yang sama seperti zona yang di-hosting lainnya dalam VPC yang sama:

"Domain yang bertentangan sudah terkait dengan VPC atau Set Delegasi yang diberikan".

Misalnya, jika zona A yang dihosting dan zona B yang dihosting keduanya memiliki nama domain yang sama, misalnya `example.com`, Anda tidak dapat mengaitkan kedua zona yang dihosting dengan VPC yang sama.

8. Pilih Buat zona yang di-hosting.

Mencantumkan zona yang di-hosting privat

Anda dapat menggunakan konsol Amazon Route 53 untuk mencantumkan semua zona yang dihosting yang Anda buat dengan AWS akun saat ini. Untuk informasi tentang cara mencantumkan zona yang dihosting menggunakan API Route 53, lihat [ListHostedZones](#) di Referensi API Amazon Route 53.

Untuk membuat daftar zona yang dihosting yang terkait dengan AWS akun

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.

Halaman Zona yang Dihosting secara otomatis menampilkan daftar semua zona yang dihosting yang dibuat menggunakan AWS akun saat ini. Kolom Jenis menunjukkan apakah zona yang di-

hosting adalah privat atau publik. Pilih judul kolom untuk mengelompokkan semua zona yang di-hosting privat dan semua zona yang di-hosting publik.

Mengaitkan lebih banyak VPCs dengan zona yang dihosting pribadi

Anda dapat menggunakan konsol Amazon Route 53 untuk mengaitkan lebih banyak VPCs dengan zona host pribadi jika Anda membuat zona yang dihosting dan VPCs dengan menggunakan AWS akun yang sama.

Important

Jika Anda ingin mengaitkan VPCs yang Anda buat dengan menggunakan satu akun dengan zona host pribadi yang Anda buat dengan menggunakan akun lain, Anda harus terlebih dahulu mengotorisasi asosiasi tersebut. Selain itu, Anda tidak dapat menggunakan AWS konsol untuk mengotorisasi asosiasi atau mengaitkannya VPCs dengan zona yang dihosting. Untuk informasi selengkapnya, lihat [Mengaitkan VPC Amazon dan zona host pribadi yang Anda buat dengan akun berbeda AWS](#).

Untuk informasi tentang cara mengaitkan lebih lanjut VPCs dengan zona yang dihosting pribadi menggunakan API Route 53, lihat [Mengaitkan VPCWith HostedZone](#) di Referensi API Amazon Route 53.

Untuk mengaitkan tambahan VPCs dengan zona host pribadi menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih tombol radio untuk zona host pribadi yang ingin Anda kaitkan lebih banyak VPCs .
4. Pilih Edit.
5. Pilih Tambah VPC.
6. Pilih Wilayah dan ID VPC yang ingin Anda kaitkan dengan zona yang di-hosting ini.
7. Untuk mengaitkan lebih banyak VPCs dengan zona yang dihosting ini, ulangi langkah 5 dan 6.
8. Pilih Simpan perubahan.

Mengaitkan VPC Amazon dan zona host pribadi yang Anda buat dengan akun berbeda AWS

Jika Anda ingin mengaitkan VPC yang Anda buat dengan satu AWS akun dengan zona host pribadi yang Anda buat dengan akun lain, lakukan prosedur berikut:

Untuk mengaitkan VPC Amazon dan zona host pribadi yang Anda buat dengan akun berbeda AWS

1. Dengan akun yang membuat zona yang di-hosting, otorisasi pengaitan VPC dengan zona yang di-hosting privat menggunakan salah satu metode berikut:
 - AWS CLI— Lihat [create-vpc-association-authorization](#) di Referensi AWS CLI Perintah
 - AWS SDK atau AWS Tools for Windows PowerShell— Lihat dokumentasi yang berlaku di halaman [AWS Dokumentasi](#)
 - Amazon Route 53 API - Lihat [Membuat VPCAssociation Otorisasi](#) di Referensi API Amazon Route 53

Perhatikan hal-hal berikut:

- Jika Anda ingin mengaitkan beberapa VPCs yang Anda buat dengan satu akun dengan zona host yang Anda buat dengan akun berbeda, Anda harus mengirimkan satu permintaan otorisasi untuk setiap VPC.
 - Ketika mengotorisasi pengaitan, Anda harus menentukan ID zona yang di-hosting, maka dari itu zona yang di-hosting privat harus sudah ada.
 - Anda tidak dapat menggunakan konsol Route 53 untuk mengotorisasi pengaitan VPC dengan zona yang di-hosting privat atau untuk membuat pengaitan.
2. Menggunakan akun yang membuat VPC, kaitkan VPC dengan zona yang di-hosting. Seperti halnya mengotorisasi asosiasi, Anda dapat menggunakan AWS SDK, Tools for Windows PowerShell, the AWS CLI, atau Route 53 API. Jika Anda menggunakan API, gunakan VPCWith HostedZone tindakan [Associate](#).
 3. Direkomendasikan – Menghapus otorisasi untuk mengaitkan VPC dengan zona yang di-hosting. Menghapus otorisasi tidak memengaruhi pengaitan, ini hanya mencegah Anda agar tidak mengaitkan ulang VPC dengan zona yang di-hosting di masa mendatang. Jika ingin mengaitkan ulang VPC dengan zona yang di-hosting, Anda harus mengulangi langkah 1 dan 2 dari prosedur ini.

⚠ Important

ListHostedZonesByVPC mengembalikan zona yang dihosting yang diberikan VPC dan GetHostedZone API mengembalikan zona yang VPCs terkait dengan zona yang dihosting. Ini APIs hanya mempertimbangkan zona yang dihosting ke asosiasi VPC yang dibuat oleh AssociateVPCWithHostedZone API atau saat zona host pribadi dibuat. Jika Anda ingin daftar lengkap asosiasi zona yang dihosting ke VPC, hubungi juga. [ListProfileResourceAssociations](#)

ℹ Note

Untuk jumlah maksimum otorisasi yang dapat Anda buat, lihat [Kuota pada entitas](#).

Memutuskan hubungan VPCs dari zona yang dihosting pribadi

Anda dapat menggunakan konsol Amazon Route 53 untuk memisahkan diri VPCs dari zona host pribadi. Tindakan ini membuat Route 53 menghentikan perutean lalu lintas menggunakan catatan di zona yang di-hosting untuk kueri DNS yang berasal dari VPC. Sebagai contoh, jika zona yang di-hosting privat example.com dikaitkan dengan VPC dan Anda memisahkan zona yang di-hosting dari VPC tersebut, Route 53 berhenti menyelesaikan kueri DNS untuk example.com atau salah satu catatan lainnya di zona yang di-hosting example.com.

ℹ Note

Anda tidak dapat memisahkan VPC terakhir dari zona yang di-hosting privat. Jika ingin memisahkan VPC, Anda terlebih dahulu harus mengaitkan VPC lain dengan zona yang di-hosting.

Untuk memisahkan diri VPCs dari zona yang dihosting pribadi

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih tombol radio untuk zona host pribadi yang ingin Anda lepaskan satu atau lebih VPCs .

4. Pilih Edit.
5. Pilih Hapus VPC di sebelah VPC yang Anda ingin pisahkan dari zona yang di-hosting.
6. Pilih Simpan perubahan.

Menghapus zona yang di-hosting privat

Bagian ini menjelaskan cara menghapus zona yang di-hosting privat menggunakan konsol Amazon Route 53.

Anda dapat menghapus zona yang di-hosting privat hanya jika tidak ada catatan selain catatan SOA dan NS default. Jika zona yang di-hosting berisi catatan lain, Anda harus menghapusnya sebelum Anda dapat menghapus zona yang di-hosting. Hal ini mencegah Anda agar tidak menghapus zona yang di-hosting yang masih berisi catatan secara tidak sengaja.

Topik

- [Menghapus zona yang di-hosting privat yang dibuat oleh layanan lain](#)
- [Menggunakan konsol Route 53 untuk menghapus zona yang di-hosting privat](#)

Menghapus zona yang di-hosting privat yang dibuat oleh layanan lain

Jika zona yang di-hosting privat dibuat oleh layanan lain, Anda tidak dapat menghapusnya menggunakan konsol Route 53. Sebagai gantinya, Anda perlu menggunakan proses yang berlaku untuk layanan lainnya:

- **AWS Cloud Map**— Untuk menghapus zona host yang AWS Cloud Map dibuat saat Anda membuat namespace DNS pribadi, hapus namespace. AWS Cloud Map menghapus zona yang dihosting secara otomatis. Untuk informasi selengkapnya, lihat [Menghapus namespace](#) di Panduan Developer AWS Cloud Map .
- **Penemuan Layanan Amazon Elastic Container Service (Amazon ECS)** – Untuk menghapus zona yang di-hosting privat yang dibuat Amazon ECS ketika Anda membuat layanan menggunakan penemuan layanan, hapus layanan Amazon ECS yang menggunakan namespace, dan hapus namespace. Untuk informasi lebih lanjut, lihat [Menghapus layanan](#) dalam Panduan Developer Amazon Elastic Container Service.

Menggunakan konsol Route 53 untuk menghapus zona yang di-hosting privat

Untuk menggunakan konsol Route 53 guna menghapus zona yang di-hosting privat, lakukan prosedur berikut.

Cara menghapus zona yang di-hosting privat menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Mengonfirmasi bahwa zona yang di-hosting yang ingin Anda hapus hanya berisi catatan NS dan SOA. Jika berisi catatan tambahan, hapuslah:
 - a. Pilih nama zona yang di-hosting yang ingin Anda hapus.
 - b. Pada halaman Catatan, jika daftar catatan termasuk catatan dengan nilai selain NS atau SOA pada kolom Jenis, pilih baris, dan pilih Hapus.

Untuk memilih beberapa catatan berturut-turut, pilih baris pertama, tekan dan tahan tombol Shift, dan pilih baris terakhir. Untuk memilih beberapa catatan tidak berturut-turut, pilih baris pertama, tekan dan tahan tombol Ctrl, dan pilih baris yang tersisa.

3. Di halaman Zona yang Di-hosting, pilih baris zona yang di-hosting yang ingin Anda hapus.
4. Pilih Hapus.
5. Ketik kunci konfirmasi dan pilih Hapus.

Izin VPC

[Izin VPC menggunakan kondisi kebijakan Manajemen Identitas dan Akses \(IAM\) untuk memungkinkan Anda menyetel izin terperinci VPCs saat menggunakan Associate, Disassociate VPCWith HostedZone, Create VPCAssociation Authorization, Delete VPCFrom HostedZone Authorization, dan VPC. VPCAssociation CreateHostedZoneListHostedZonesBy APIs](#)

Dengan kondisi kebijakan IAM `route53:VPCs`, Anda dapat memberikan hak administratif terperinci kepada pengguna lain AWS. Ini memungkinkan Anda memberikan izin kepada seseorang untuk mengaitkan zona yang dihosting dengan, memisahkan zona yang dihosting dari, membuat otorisasi asosiasi VPC untuk, menghapus otorisasi asosiasi VPC untuk, membuat zona yang dihosting dengan atau mencantumkan zona yang dihosting untuk:

- Sebuah VPC tunggal.
- Semua orang VPCs dalam wilayah yang sama.

- Berganda VPCs.

Untuk informasi selengkapnya tentang izin VPC, lihat [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#)

Untuk mempelajari cara mengautentikasi AWS pengguna, lihat [Mengautentikasi dengan identitas](#) dan mempelajari cara mengontrol akses ke sumber daya Route 53, lihat [Kontrol akses](#).

Migrasi zona yang dihosting ke akun lain AWS

Saat memigrasikan zona yang dihosting ke zona lain Akun AWS, ikuti langkah-langkah yang disarankan ini.

Langkah-langkah ini paling cocok untuk zona yang dihosting dengan perubahan catatan yang jarang terjadi. Untuk zona yang dihosting dengan pembaruan rekaman yang sering, pertimbangkan hal berikut:

- Jangan memperbarui catatan sumber daya apa pun selama migrasi.
- Publikasikan perubahan catatan sumber daya di zona host lama dan baru setelah delegasi ditransfer.

Prasyarat

Instal atau tingkatkan AWS CLI:

Untuk informasi tentang mengunduh, menginstal, dan mengonfigurasi AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#).

Note

Mengkonfigurasi CLI agar Anda dapat menggunakannya ketika menggunakan akun yang membuat zona yang di-hosting dan akun yang dimigrasi ke zona yang di-hosting. Untuk informasi selengkapnya, lihat [Konfigurasi](#) dalam Panduan Pengguna AWS Command Line Interface

Jika Anda sudah menggunakan AWS CLI, kami sarankan Anda meningkatkan ke versi terbaru CLI sehingga perintah CLI mendukung fitur Route 53 terbaru.

Topik

- [Langkah 1: Bersiaplah untuk Migrasi](#)
- [Langkah 2: Membuat zona yang di-hosting baru](#)
- [Langkah 3: \(Opsional\) Migrasikan pemeriksaan kesehatan](#)
- [Langkah 4: Migrasikan catatan dari zona host lama ke zona host baru](#)
- [Langkah 5: Bandingkan catatan di zona host lama dan baru](#)
- [Langkah 6: Perbarui pendaftaran domain untuk menggunakan server nama untuk zona host baru](#)
- [Langkah 7: Ubah TTL untuk catatan NS kembali ke nilai yang lebih tinggi](#)
- [Langkah 8: Aktifkan kembali penandatanganan DNSSEC dan buat rantai kepercayaan \(jika diperlukan\)](#)
- [Langkah 9: \(Opsional\) hapus zona host lama](#)

Langkah 1: Bersiaplah untuk Migrasi

Langkah-langkah persiapan membantu Anda meminimalkan risiko yang terkait dengan migrasi zona yang dihosting.

1. Memantau ketersediaan zona

Anda dapat memantau zona untuk ketersediaan nama domain Anda. Ini dapat membantu Anda mengatasi masalah apa pun yang mungkin menyebabkan pengembalian migrasi. Anda dapat memantau nama domain Anda dengan sebagian besar lalu lintas dengan menggunakan CloudWatch atau melakukan pencatatan kueri. Untuk informasi selengkapnya tentang menyiapkan pencatatan kueri, lihat [Memantau Amazon Route 53](#).

Pemantauan dapat dilakukan melalui skrip shell, atau melalui layanan pihak ketiga. Namun, seharusnya tidak menjadi satu-satunya sinyal untuk menentukan apakah rollback diperlukan karena Anda mungkin juga mendapatkan umpan balik dari pelanggan Anda karena domain tidak tersedia.

2. Turunkan pengaturan TTL

Pengaturan TTL (waktu untuk tayang) bagi catatan menentukan durasi penyelesai DNS untuk meng-cache catatan dan menggunakan informasi yang di-cache. Ketika TTL berakhir, penyelesai mengirimkan kueri lain ke penyedia layanan DNS untuk domain guna mendapatkan informasi terbaru.

Pengaturan TTL khas untuk catatan NS adalah 172800 detik, atau dua hari. Catatan NS mencantumkan server nama yang dapat digunakan Sistem Nama Domain (DNS) untuk mendapatkan informasi tentang cara merutekan lalu lintas domain Anda. Menurunkan TTL untuk catatan NS, baik dengan penyedia layanan DNS Anda saat ini maupun dengan Route 53, mengurangi waktu henti untuk domain Anda jika Anda menemukan masalah saat Anda memigrasikan DNS ke Route 53. Jika Anda tidak menurunkan TTL, domain mungkin tidak tersedia di internet hingga dua hari jika terjadi kesalahan.

Untuk menurunkan TTL

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pilih Zona yang dihosting di panel navigasi.
3. Pilih nama zona yang di-hosting.
4. Pilih catatan NS, dan di panel Record details, pilih Edit record.
5. Mengubah nilai TTL (Detik). Kami rekomendasikan Anda menentukan nilai antara 60 detik hingga 900 detik (15 menit).
6. Pilih Simpan.

3. Hapus catatan DS dari zona induk (Jika Anda memiliki DNSSEC dikonfigurasi)

Jika Anda telah mengonfigurasi DNSSEC untuk domain, hapus catatan Delegation Signer (DS) dari zona induk sebelum memigrasi domain ke Route 53.

Jika zona induk di-host melalui Route 53, lihat [Menghapus kunci publik untuk domain](#) untuk informasi selengkapnya. Jika zona induk di-host di registrar lain, hubungi mereka untuk menghapus catatan DS.

Route 53 saat ini tidak mendukung migrasi setelah DNSSEC. Dengan demikian, Anda harus menonaktifkan validasi DNSSEC yang dilakukan terhadap domain Anda sebelum migrasi dengan menghapus catatan DS dari zona induk. Setelah migrasi, Anda dapat mengaktifkan kembali validasi DNSSEC dengan mengonfigurasi DNSSEC di zona host baru dan menambahkan catatan DS masing-masing ke zona induk.

4. Pastikan tidak ada operasi lain yang sedang berlangsung yang bergantung pada zona host yang bermigrasi

Beberapa operasi akan bergantung pada resolusi DNS di zona host yang bermigrasi, misalnya, proses perpanjangan TLS/SSL sertifikat mungkin memerlukan perubahan catatan DNS dan penyedia akan mencoba menyelesaikan catatan DNS sebagai metode validasi. Sebelum migrasi, Anda harus memastikan tidak ada operasi lain yang terjadi, untuk menghindari dampak tak terduga dari migrasi zona yang dihosting.

Langkah 2: Membuat zona yang di-hosting baru

Buat zona host baru di akun tempat Anda ingin memigrasikan zona yang dihosting.

Pilih tab untuk instruksi untuk konsol AWS CLI atau konsol.

- [CLI](#)
- [Konsol](#)

CLI

Masukkan perintah berikut:

```
aws route53 create-hosted-zone \  
    --name $hosted_zone_name \  
    --caller-reference $unique_string
```

Untuk informasi selengkapnya, lihat [create-hosted-zone](#).

Console

Cara membuat zona yang di-hosting baru menggunakan akun yang berbeda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Masuk dengan kredensial akun untuk akun yang ingin dimigrasi ke zona yang di-hosting.

2. Membuat zona yang di-hosting. Untuk informasi selengkapnya, lihat [Membuat zona yang di-hosting publik](#).
3. Catat ID zona yang di-hosting. Dalam beberapa kasus, Anda akan memerlukan informasi ini nanti dalam prosesnya.
4. Keluar dari konsol Route 53.

Turunkan NS TTL di zona baru juga, mirip dengan pengaturan TTL Bawah dalam persiapan Langkah 1, Turunkan pengaturan TTL.

Langkah 3: (Opsional) Migrasikan pemeriksaan kesehatan

Anda dapat mengaitkan catatan DNS di akun baru dengan pemeriksaan kesehatan Route 53 dari akun tempat Anda bermigrasi. Untuk memigrasikan pemeriksaan kesehatan Route 53, Anda perlu membuat pemeriksaan kesehatan baru di akun baru Anda dengan konfigurasi yang sama dengan yang sudah ada. Untuk informasi selengkapnya, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

Langkah 4: Migrasikan catatan dari zona host lama ke zona host baru

Anda dapat memigrasikan rekaman dari satu Akun AWS ke yang lain dengan menggunakan konsol atau file. AWS CLI

Console

Jika zona Anda hanya berisi beberapa catatan, Anda dapat mempertimbangkan untuk menggunakan konsol Route 53 untuk mencantumkan catatan di zona lama Anda, mencatatnya, dan membuatnya di zona baru. Jika Anda telah memigrasikan pemeriksaan kesehatan [Langkah 3: \(Opsional\) Migrasikan pemeriksaan kesehatan](#), saat membuat catatan di zona host baru, Anda harus menentukan ID pemeriksaan kesehatan baru. Untuk informasi selengkapnya, lihat topik berikut:

- [Mencantumkan catatan](#)
- [Membuat catatan dengan menggunakan konsol Amazon Route 53](#)
- [Mengonfigurasi failover DNS](#)

Anda harus menurunkan NS TTL di zona baru juga, mirip dengan pengaturan TTL Bawah di Langkah 1.

CLI

Jika zona Anda berisi sejumlah besar catatan, Anda dapat mengekspor catatan yang ingin Anda migrasi ke file, mengedit file, dan kemudian menggunakan file yang diedit untuk membuat catatan di zona host baru. Prosedur berikut menggunakan perintah AWS CLI, meskipun alat pihak ketiga juga tersedia untuk tujuan ini.

1. Jalankan perintah berikut:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

Perhatikan hal-hal berikut:

- Untuk *hosted-zone-id*, tentukan ID zona host lama yang berisi catatan yang ingin Anda migrasi.
- Untuk *path-to-output-file*, tentukan jalur direktori dan nama file tempat Anda ingin menyimpan outputnya.
- Karakter > mengirimkan output ke file yang ditentukan.
- AWS CLI Secara otomatis menangani pagination untuk zona yang dihosting yang berisi lebih dari 100 catatan. Untuk informasi selengkapnya, lihat [Menggunakan opsi pagination Antarmuka Baris AWS Perintah](#) di Panduan AWS Command Line Interface Pengguna.

Jika Anda menggunakan metode terprogram lain untuk membuat daftar catatan, seperti salah satunya AWS SDKs, Anda bisa mendapatkan maksimal 100 catatan per halaman hasil. Jika zona yang di-hosting berisi lebih dari 100 catatan, Anda harus mengirimkan beberapa permintaan untuk mencantumkan semua catatan.

Buat salinan output ini. Setelah Anda membuat catatan di zona host baru, kami sarankan Anda menjalankan AWS CLI `list-resource-record-sets` perintah di zona host baru dan membandingkan dua output untuk memastikan bahwa semua catatan dibuat.

2. Edit catatan yang ingin Anda migrasikan.

Edit file yang diekspor sebelum Anda dapat menggunakannya dengan `change-resource-record-sets` perintah. Anda dapat membuat perubahan ini menggunakan fungsi pencarian dan ganti di editor teks.

Note

Langkah-langkah berikut menjelaskan pengeditan manual menggunakan editor teks. Pengguna tingkat lanjut dapat mengotomatiskan transformasi ini menggunakan alat terprogram seperti jq, Python, atau bahasa scripting lainnya.

Buka salinan file yang Anda buat di langkah 1 prosedur ini yang berisi catatan yang ingin Anda migrasi, dan buat perubahan berikut:

- Ganti ResourceRecordSets elemen di bagian atas file dengan Changes elemen.
- Opsional - menambahkan Comment elemen.
- Hapus baris yang terkait dengan catatan NS dan SOA dari nama zona yang dihosting. zona yang di-hosting baru sudah memiliki catatan tersebut.
- Untuk setiap catatan, tambahkan ResourceRecordSets elemen Action dan, tambahkan tanda kurung pembuka dan penutup ({ }) sesuai kebutuhan untuk membuat kode JSON valid.

 Note

Anda dapat menggunakan validator JSON untuk memverifikasi bahwa semua tanda kurung ada di tempat yang benar. Untuk menemukan validator JSON online, cari “validator JSON” di browser Anda.

- Jika zona yang di-hosting berisi alias yang merujuk ke catatan lain di zona yang di-hosting yang sama, buat perubahan berikut:
 - Ubah ID zona yang di-hosting menjadi ID zona yang di-hosting baru.

 Important

Jika catatan alias menunjuk ke sumber daya lain, misalnya penyeimbang beban, jangan ubah ID zona yang dihosting ke ID zona yang dihosting domain. Jika Anda mengubah ID zona yang dihosting secara tidak sengaja, kembalikan ID zona yang dihosting ke id zona yang dihosting dari sumber daya itu sendiri, bukan ID zona yang dihosting dari domain tersebut. ID zona yang dihosting sumber daya dapat ditemukan di AWS konsol tempat sumber daya dibuat.

- Pindahkan catatan alias ke bagian bawah file. Route 53 harus membuat catatan yang dirujuk catatan alias sebelum dapat membuat catatan alias.

 Important

Jika satu atau lebih catatan alias merujuk ke catatan alias lain, catatan yang merupakan target alias harus muncul dalam file sebelum mereferensi catatan alias. Misalnya, jika `alias.example.com` adalah target alias untuk `alias.alias.example.com`, `alias.example.com` harus muncul terlebih dahulu di file.

- Hapus catatan alias yang merutekan lalu lintas ke instans kebijakan lalu lintas. Catat catatan tersebut agar Anda dapat membuatnya lagi nanti.
- Jika Anda memigrasikan pemeriksaan kesehatan [Langkah 3: \(Opsional\) Migrasikan pemeriksaan kesehatan](#), ubah catatan untuk dikaitkan dengan pemeriksaan IDs kesehatan yang baru dibuat.

Contoh berikut menunjukkan versi catatan yang diedit untuk zona yang di-hosting bagi `example.com`. Teks merah dan dicetak miring adalah yang baru:

```
{  
  "Comment": "string",  
  "Changes": [  
    {  
      "Action": "CREATE",  
      "ResourceRecordSet": {  
        "ResourceRecords": [  
          {  
            "Value": "192.0.2.4"  
          },  
          {  
            "Value": "192.0.2.5"  
          },  
          {  
            "Value": "192.0.2.6"  
          }  
        ],  
        "Type": "A",  
        "Name": "route53documentation.com.",  
        "TTL": 300  
      }  
    },  
  ],  
}
```

```

{
  "Action": "CREATE",
  "ResourceRecordSet": {
    "AliasTarget": {
      "HostedZoneId": "Z3BJ6K6RIION7M",
      "EvaluateTargetHealth": false,
      "DNSName": "s3-website-us-west-2.amazonaws.com."
    },
    "Type": "A",
    "Name": "www.route53documentation.com."
  }
}

```

3. Membagi file besar menjadi file yang lebih kecil

Jika Anda memiliki banyak catatan atau jika Anda memiliki catatan dengan banyak nilai (misalnya, banyak alamat IP), Anda mungkin perlu membagi file menjadi file yang lebih kecil. Nilai maksnya adalah:

- Setiap file dapat berisi maksimum 1.000 catatan.
- Panjang nilai gabungan maksimum dalam semua elemen `Value` adalah 32.000 byte.

4. Buat catatan di zona host baru

Masukkan CLI berikut:

```

aws route53 change-resource-record-sets \
  --hosted-zone-id new-hosted-zone-id \
  --change-batch file://path-to-file-that-contains-records

```

Tentukan nilai-nilai berikut ini:

- Untuk *new-hosted-zone-id*, tentukan ID zona host baru.
- Untuk *path-to-file-that-contains-records*, tentukan jalur direktori dan nama file yang Anda edit di langkah sebelumnya.

Jika Anda menghapus catatan alias yang merutekan lalu lintas ke instans kebijakan lalu lintas, buat ulang catatan alias menggunakan konsol Route 53. Untuk informasi selengkapnya, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#).

Langkah 5: Bandingkan catatan di zona host lama dan baru

Untuk mengonfirmasi bahwa Anda berhasil membuat semua catatan Anda di zona host baru, masukkan perintah CLI berikut untuk membuat daftar catatan di zona host baru dan bandingkan output dengan daftar catatan dari zona host lama.

```
aws route53 list-resource-record-sets \  
    --hosted-zone-id new-hosted-zone-id \  
    --output json > path-to-output-file
```

Tentukan nilai-nilai berikut ini:

- Untuk *new-hosted-zone-id*, tentukan ID zona host baru.
- Untuk *path-to-output-file*, tentukan jalur direktori dan nama file tempat Anda ingin menyimpan outputnya. Gunakan nama file yang berbeda dari nama file yang Anda gunakan di Langkah 4.

Karakter > mengirimkan output ke file yang ditentukan.

Bandinkan output dengan output dari Langkah 4. Selain nilai catatan NS dan SOA dan perubahan apa pun yang Anda buat di Langkah 4 (seperti zona host IDs atau nama domain yang berbeda), kedua output harus identik.

Jika catatan di zona host baru tidak cocok dengan catatan di zona host lama, lakukan salah satu hal berikut:

- Buat koreksi kecil menggunakan konsol Route 53. Untuk informasi selengkapnya, lihat [Mengedit catatan](#).
- Hapus semua catatan kecuali catatan NS dan SOA di zona host baru, dan ulangi prosedur di Langkah 4.

Langkah 6: Perbarui pendaftaran domain untuk menggunakan server nama untuk zona host baru

Setelah Anda selesai memigrasikan catatan ke zona host baru, ubah server nama untuk pendaftaran domain untuk menggunakan server nama untuk zona host baru. Untuk informasi selengkapnya, lihat [Menetapkan Amazon Route 53 sebagai layanan DNS untuk domain yang ada](#).

Jika zona host Anda sedang digunakan - misalnya, jika pengguna Anda menggunakan nama domain untuk menjelajah ke situs web atau mengakses aplikasi web - Anda harus terus memantau lalu lintas dan ketersediaan zona yang dihosting, termasuk lalu lintas situs web atau aplikasi, email, dll.

- Jika lalu lintas melambat atau berhenti — Ubah layanan nama untuk pendaftaran domain kembali ke server nama sebelumnya dari zona host lama. Kemudian tentukan apa yang salah.
- Jika lalu lintas tidak terpengaruh — Lanjutkan ke langkah berikutnya.

Langkah 7: Ubah TTL untuk catatan NS kembali ke nilai yang lebih tinggi

Di zona host baru, ubah TTL untuk catatan NS ke nilai yang lebih khas, misalnya, 172800 detik (dua hari). Hal ini meningkatkan latensi untuk pengguna Anda karena mereka tidak harus sering menunggu penyelesaian DNS mengirim kueri bagi server nama untuk domain Anda.

Untuk mengubah TTL

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pilih Zona yang dihosting di panel navigasi.
3. Pilih nama zona yang di-hosting.
4. Pilih catatan NS, dan di panel Record details, pilih Edit record.
5. Ubah nilai TTL (Seconds) ke jumlah detik yang Anda inginkan DNS resolver untuk cache nama-nama server nama untuk domain Anda. Kami merekomendasikan nilai 172800 detik.
6. Pilih Simpan.

Langkah 8: Aktifkan kembali penandatanganan DNSSEC dan buat rantai kepercayaan (jika diperlukan)

Anda dapat mengaktifkan kembali penandatanganan DNSSEC dalam dua langkah:

1. Aktifkan penandatanganan DNSSEC untuk Route 53, dan minta Route 53 membuat kunci penandatanganan kunci (KSK) berdasarkan kunci yang dikelola pelanggan. AWS Key Management Service
2. Buat rantai kepercayaan untuk zona yang dihosting dengan menambahkan catatan Delegation Signer (DS) ke zona induk, sehingga respons DNS dapat diautentikasi dengan tanda tangan kriptografi tepercaya.

Untuk petunjuk, lihat [Mengaktifkan penandatanganan DNSSEC dan membuat rantai kepercayaan](#).

Langkah 9: (Opsional) hapus zona host lama

Ketika Anda yakin bahwa zona yang di-hosting lama tidak lagi diperlukan, Anda memiliki opsi untuk menghapusnya. Untuk petunjuk, lihat [Menghapus zona yang di-hosting publik](#).

Important

Jangan hapus zona yang di-hosting lama atau catatan di zona yang di-hosting tersebut setidaknya 48 jam setelah Anda memperbarui pendaftaran domain untuk menggunakan server nama bagi zona yang di-hosting baru. Jika Anda menghapus zona yang di-hosting lama sebelum penyelesai DNS berhenti menggunakan catatan di zona yang di-hosting tersebut, domain Anda mungkin tidak tersedia di internet hingga penyelesai mulai menggunakan zona yang di-hosting baru.

Bekerja dengan catatan

Setelah Anda membuat zona yang di-hosting untuk domain Anda, seperti example.com, Anda membuat catatan untuk memberi tahu Domain Name System (DNS) bagaimana Anda ingin lalu lintas dirutekan untuk domain tersebut.

Misalnya, Anda mungkin membuat catatan yang menyebabkan DNS melakukan hal berikut:

- Rutekan lalu lintas internet misalnya.com ke alamat IP host di pusat data Anda.
- Rutekan email untuk domain tersebut (ichiro@example.com) ke server email (mail.example.com).
- Rutekan lalu lintas untuk subdomain yang disebut operations.tokyo.example.com ke alamat IP dari host yang berbeda.

Setiap catatan mencakup nama domain atau subdomain, jenis catatan (misalnya, catatan dengan jenis email rute MX), dan informasi lain yang berlaku untuk jenis catatan (untuk data MX, nama host dari satu atau lebih server surat dan prioritas untuk setiap server). Untuk informasi selengkapnya tentang berbagai jenis catatan, lihat [Tipe data DNS yang didukung](#).

Nama setiap catatan di zona yang di-hosting harus diakhiri dengan nama zona yang di-hosting. Misalnya, zona yang di-hosting example.com dapat berisi catatan untuk subdomain

www.example.com dan accounting.tokyo.example.com, tetapi tidak dapat berisi catatan untuk subdomain www.example.ca.

Note

Untuk membuat catatan untuk konfigurasi perutean yang kompleks, Anda juga dapat menggunakan editor visual Aliran Lalu Lintas dan menyimpan konfigurasi sebagai kebijakan lalu lintas. Anda kemudian dapat mengaitkan kebijakan lalu lintas dengan satu atau lebih nama domain (seperti example.com) atau nama subdomain (seperti www.example.com), di zona yang di-hosting yang sama atau di beberapa zona yang di-hosting. Selain itu, Anda dapat memulihkan pembaruan jika konfigurasi baru tidak memiliki performa seperti yang Anda harapkan. Untuk informasi selengkapnya, lihat [Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS](#).

Amazon Route 53 tidak mengenakan biaya untuk catatan yang Anda tambahkan ke zona yang di-hosting. Untuk informasi tentang jumlah maksimum catatan yang dapat Anda buat di zona yang di-hosting, lihat [Kuota](#).

Topik

- [Memilih kebijakan perutean](#)
- [Memilih antara catatan alias dan nonalias](#)
- [Tipe data DNS yang didukung](#)
- [Membuat catatan dengan menggunakan konsol Amazon Route 53](#)
- [Izin set catatan sumber daya](#)
- [Nilai yang Anda tentukan saat membuat atau mengedit catatan Amazon Route 53](#)
- [Membuat catatan dengan mengimpor file zona](#)
- [Mengedit catatan](#)
- [Menghapus catatan](#)
- [Mencantumkan catatan](#)

Memilih kebijakan perutean

Saat Anda membuat catatan, Anda memilih kebijakan perutean, yang menentukan bagaimana Amazon Route 53 merespons kueri:

- Kebijakan perutean sederhana – Gunakan untuk satu sumber daya yang menjalankan fungsi tertentu untuk domain Anda, misalnya, server web yang menyajikan konten untuk situs web example.com. Anda dapat menggunakan perutean sederhana untuk membuat catatan di zona host pribadi.
- Kebijakan perutean failover – Gunakan ketika Anda ingin mengonfigurasi failover aktif-pasif. Anda dapat menggunakan perutean failover untuk membuat catatan di zona host pribadi.
- Kebijakan perutean geolokasi– Gunakan saat Anda ingin merutekan lalu lintas berdasarkan lokasi pengguna Anda. Anda dapat menggunakan perutean geolokasi untuk membuat catatan di zona host pribadi.
- Kebijakan perutean geoproximity - Gunakan saat Anda ingin merutekan lalu lintas berdasarkan lokasi sumber daya Anda dan, secara opsional, mengalihkan lalu lintas dari sumber daya di satu lokasi ke sumber daya di lokasi lain. Anda dapat menggunakan perutean geoproximity untuk membuat catatan di zona host pribadi.
- Kebijakan perutean latensi — Gunakan saat Anda memiliki sumber daya dalam beberapa Wilayah AWS dan Anda ingin merutekan lalu lintas ke Wilayah yang memberikan latensi terbaik. Anda dapat menggunakan perutean latensi untuk membuat catatan di zona host pribadi.
- Kebijakan perutean berbasis IP — Gunakan saat Anda ingin merutekan lalu lintas berdasarkan lokasi pengguna Anda, dan dapatkan alamat IP tempat lalu lintas berasal.
- Kebijakan perutean jawaban multinilai – Gunakan saat Anda ingin Route 53 merespons kueri DNS dengan hingga delapan catatan sehat yang dipilih secara acak. Anda dapat menggunakan routing jawaban multivalue untuk membuat catatan di zona host pribadi.
- Kebijakan perutean berbobot – Gunakan untuk merutekan lalu lintas ke beberapa sumber daya dalam proporsi yang Anda tentukan. Anda dapat menggunakan perutean tertimbang untuk membuat catatan di zona host pribadi.

Topik

- [Perutean sederhana](#)
- [Perutean failover](#)
- [Perutean geolokasi](#)
- [Perutean geoproksimitas](#)
- [Perutean berbasis latensi](#)
- [Perutean berbasis IP](#)
- [Perutean jawaban multinilai](#)

- [Perutean tertimbang](#)
- [Bagaimana Amazon Route 53 menggunakan EDNS0 untuk memperkirakan lokasi pengguna](#)

Perutean sederhana

Perutean sederhana memungkinkan Anda mengonfigurasi data DNS standar, tanpa perutean Route 53 khusus seperti tertimbang atau latensi. Dengan perutean yang sederhana, Anda biasanya mengarahkan lalu lintas ke sumber daya tunggal, misalnya, ke server web untuk situs web Anda.

Anda dapat menggunakan kebijakan perutean sederhana untuk catatan di zona host pribadi.

Jika Anda memilih kebijakan perutean sederhana di konsol Route 53, Anda tidak dapat membuat beberapa catatan yang memiliki nama dan jenis yang sama, tetapi Anda dapat menentukan beberapa nilai dalam catatan yang sama, seperti beberapa alamat IP. (Jika Anda memilih kebijakan perutean sederhana untuk catatan alias, Anda hanya dapat menentukan satu AWS sumber daya atau satu catatan di zona yang dihosting saat ini.) Jika Anda menentukan beberapa nilai dalam catatan, Route 53 mengembalikan semua nilai ke resolver rekursif dalam urutan acak, dan resolver mengembalikan nilai ke klien (seperti peramban web) yang mengirimkan kueri DNS. Klien kemudian memilih nilai dan mengirim ulang kueri. Dengan kebijakan routing sederhana, meskipun Anda dapat menentukan beberapa alamat IP, alamat IP ini tidak diperiksa kesehatan.

Untuk informasi tentang nilai yang Anda tentukan saat menggunakan kebijakan perutean sederhana untuk membuat rekaman, lihat topik berikut ini:

- [Nilai khusus untuk catatan sederhana](#)
- [Nilai khusus untuk catatan alias sederhana](#)
- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Perutean failover

Perutean failover memungkinkan Anda merutekan lalu lintas ke sumber daya saat sumber daya sehat atau ke sumber daya lain saat sumber daya pertama tidak sehat. Catatan primer dan sekunder dapat merutekan lalu lintas ke apa pun dari bucket Amazon S3 yang dikonfigurasi sebagai situs web ke pohon catatan yang kompleks. Untuk informasi selengkapnya, lihat [Failover active-passive](#).

Anda dapat menggunakan kebijakan perutean failover untuk catatan di zona host pribadi.

Untuk informasi tentang nilai yang Anda tentukan saat menggunakan kebijakan perutean failover untuk membuat catatan, lihat topik berikut ini:

- [Nilai khusus untuk catatan failover](#)
- [Nilai khusus untuk catatan alias failover](#)
- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Perutean geolokasi

Perutean geolokasi memungkinkan Anda memilih sumber daya yang melayani lalu lintas Anda berdasarkan lokasi geografis pengguna Anda, yang berarti lokasi asal kueri DNS. Misalnya, Anda mungkin ingin semua kueri dari Eropa dialihkan ke penyeimbang beban Elastic Load Balancing di Wilayah Frankfurt.

Saat Anda menggunakan perutean geolokasi, Anda dapat melokalkan konten Anda dan menyajikan beberapa atau semua situs web Anda dalam bahasa pengguna Anda. Anda juga dapat menggunakan perutean geolokasi untuk membatasi distribusi konten hanya ke lokasi di mana Anda memiliki hak distribusi. Penggunaan lain yang mungkin adalah untuk menyeimbangkan beban di seluruh titik akhir dengan easy-to-manage cara yang dapat diprediksi, sehingga setiap lokasi pengguna secara konsisten diarahkan ke titik akhir yang sama.

Anda dapat menentukan lokasi geografis menurut benua, negara, atau negara bagian di Amerika Serikat. Jika Anda membuat catatan terpisah untuk wilayah geografis yang tumpang tindih—misalnya, satu rekaman untuk Amerika Utara dan satu untuk Kanada—prioritas masuk ke wilayah geografis terkecil. Ini memungkinkan Anda untuk merutekan beberapa kueri untuk suatu benua ke satu sumber daya dan untuk merutekan kueri untuk negara yang dipilih di benua itu ke sumber daya yang berbeda. (Untuk daftar negara di setiap benua, lihat [Lokasi](#).)

Geolokasi berfungsi dengan memetakan alamat IP ke lokasi. Namun, beberapa alamat IP tidak dipetakan ke lokasi geografis, jadi meskipun Anda membuat catatan geolokasi yang mencakup ketujuh benua, Amazon Route 53 akan menerima beberapa kueri DNS dari lokasi yang tidak dapat diidentifikasi. Anda dapat membuat catatan default yang menangani kedua kueri dari alamat IP yang tidak dipetakan ke lokasi mana pun dan kueri yang berasal dari lokasi yang data geolokasinya belum Anda buat. Jika Anda tidak membuat catatan default, Route 53 menghasilkan respons "tidak ada jawaban" untuk kueri dari lokasi tersebut.

Anda dapat menggunakan perutean geolokasi untuk catatan di zona host publik dan pribadi.

Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menggunakan EDNS0 untuk memperkirakan lokasi pengguna](#).

Untuk informasi tentang nilai yang Anda tentukan saat menggunakan kebijakan perutean geolokasi untuk membuat catatan, lihat topik berikut ini:

- [Nilai khusus untuk catatan geolokasi](#)
- [Nilai khusus untuk catatan alias geolokasi](#)
- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Perutean geolokasi di zona host pribadi

Untuk zona yang dihosting pribadi, Route 53 merespons kueri DNS berdasarkan VPC Wilayah AWS tempat kueri tersebut berasal. Untuk daftar Wilayah AWS, lihat [Wilayah dan zona](#) di panduan EC2 pengguna Amazon.

Jika kueri DNS berasal dari bagian lokal dari jaringan hybrid, itu akan dianggap berasal dari tempat VPC berada. Wilayah AWS

Jika menyertakan pemeriksaan kesehatan, Anda dapat membuat catatan default untuk:

- Alamat IP yang tidak dipetakan ke lokasi geografis.
- Kueri DNS yang berasal dari lokasi yang belum Anda buat catatan geolokasi.

Jika catatan geolokasi untuk wilayah kueri DNS tidak sehat, catatan default akan dikembalikan (jika sehat).

Dalam konfigurasi contoh pada gambar berikut, kueri DNS yang berasal dari us-east-1 Wilayah AWS (Virginia) akan dialihkan ke titik akhir 1.1.1.1.

Quick create record [Info](#) [Switch to wizard](#)

▼ Record 1 Delete

Record name [Info](#)
 .demo.com
Keep blank to create a record for the root domain.

Record type [Info](#)

A – Routes traffic to an IPv4 address and some resources ▼

Value [Info](#) ☒ Alias

Enter multiple values on separate lines.

TTL (seconds) [Info](#)
Recommended values: 60 to 172800 (two days)

Routing policy [Info](#)

Geolocation ▼

Location

Virginia ▼

Health check ID - optional [Info](#)

Perutean geoproksimitas

Perutean geoproximity memungkinkan Amazon Route 53 merutekan lalu lintas ke sumber daya Anda berdasarkan lokasi geografis pengguna dan sumber daya Anda. Ini merutekan lalu lintas ke sumber daya terdekat yang tersedia. Anda juga dapat memilih untuk mengarahkan lebih banyak lalu lintas atau lebih sedikit lalu lintas ke sumber daya tertentu dengan menentukan nilai, yang dikenal sebagai bias. Bias memperluas atau mengecilkan ukuran wilayah geografis tempat lalu lintas dirutekan ke sumber daya.

Anda membuat aturan geoproximity untuk sumber daya Anda dan menentukan salah satu nilai berikut untuk setiap aturan:

- Jika Anda menggunakan AWS sumber daya, tentukan Wilayah AWS atau Grup Zona Lokal tempat Anda membuat sumber daya.
- Jika Anda menggunakan AWS non-sumber daya, tentukan garis lintang dan bujur sumber daya.

Untuk menggunakan AWS Local Zones, Anda harus mengaktifkannya terlebih dahulu. Untuk informasi selengkapnya, lihat [Memulai Local Zones](#) di Panduan Pengguna AWS Local Zones.

Untuk mempelajari perbedaan antara Wilayah AWS dan Local Zones, lihat [Wilayah dan Zona](#) di Panduan EC2 Pengguna Amazon.

Memilih kebijakan perutean

Versi API 2013-04-01 591

Untuk mengubah ukuran wilayah geografis dari mana Route 53 route lalu lintas ke sumber daya, tentukan nilai yang berlaku untuk bias:

- Untuk memperluas ukuran wilayah geografis tempat Route 53 merutekan lalu lintas ke sumber daya, tentukan bilangan bulat positif dari 1 hingga 99 untuk bias. Route 53 menyusutkan ukuran wilayah yang berdekatan.
- Untuk menyusutkan ukuran wilayah geografis yang lalu lintasnya dirutekan oleh Route 53 ke sumber daya, tentukan bias negatif -1 sampai -99. Route 53 memperluas ukuran wilayah yang berdekatan.

 Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

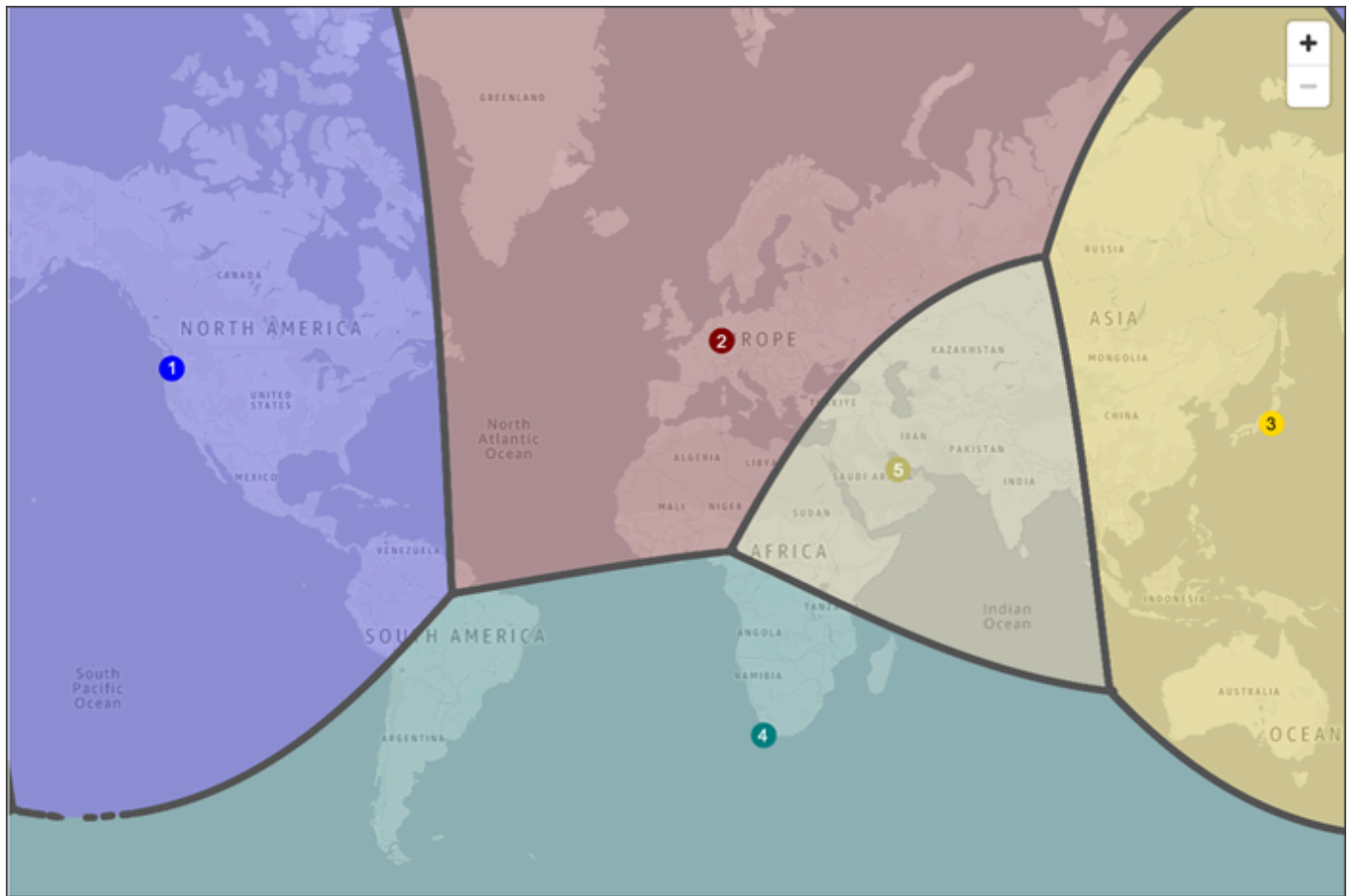
New console

Peta berikut menunjukkan empat Wilayah AWS (nomor 1 sampai 5):

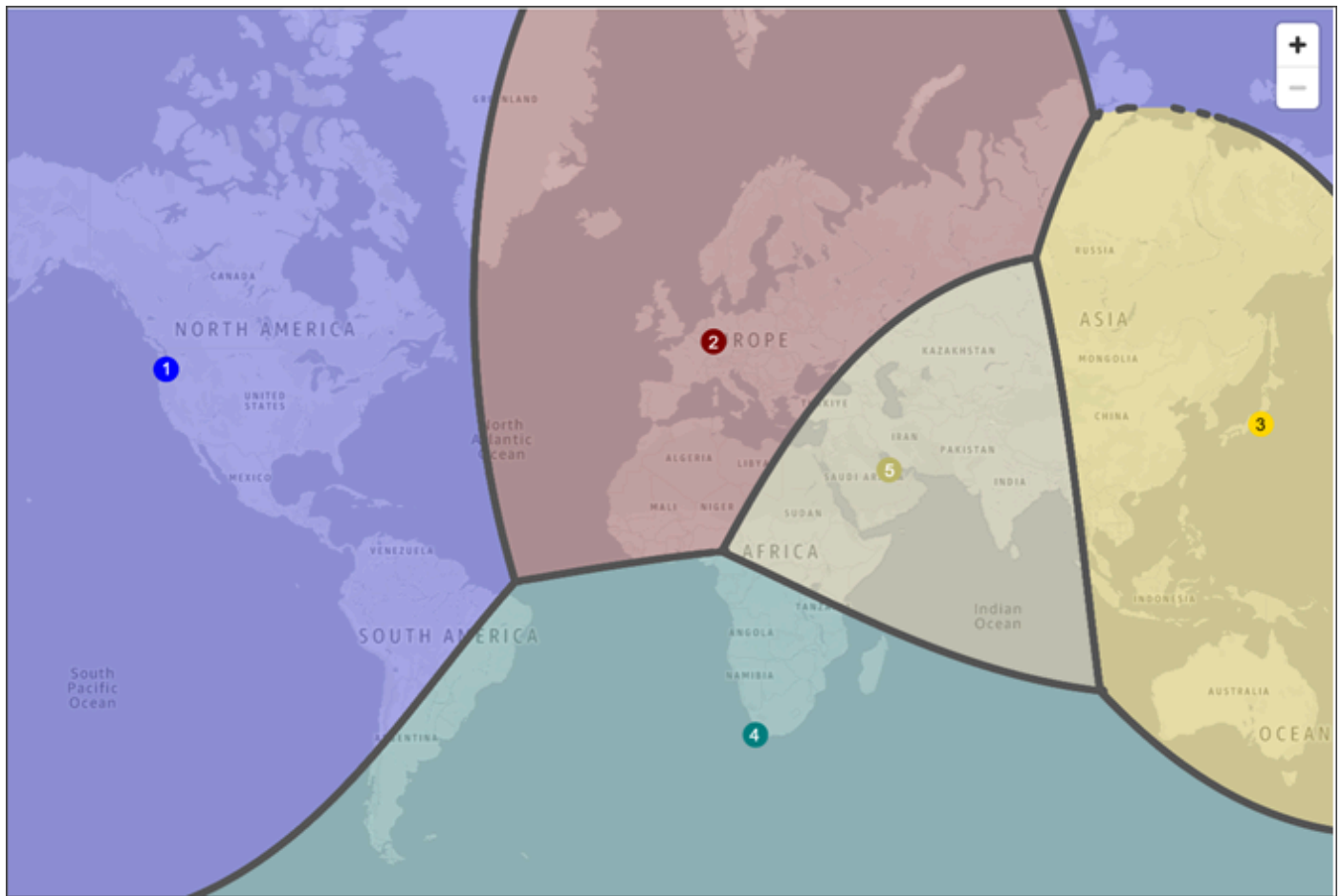
1. AS Barat (Oregon)
2. Eropa (Frankfurt)
3. Asia Pasifik (Tokyo)
4. Africa (Cape Town)
5. Timur Tengah (Bahrain)

 Note

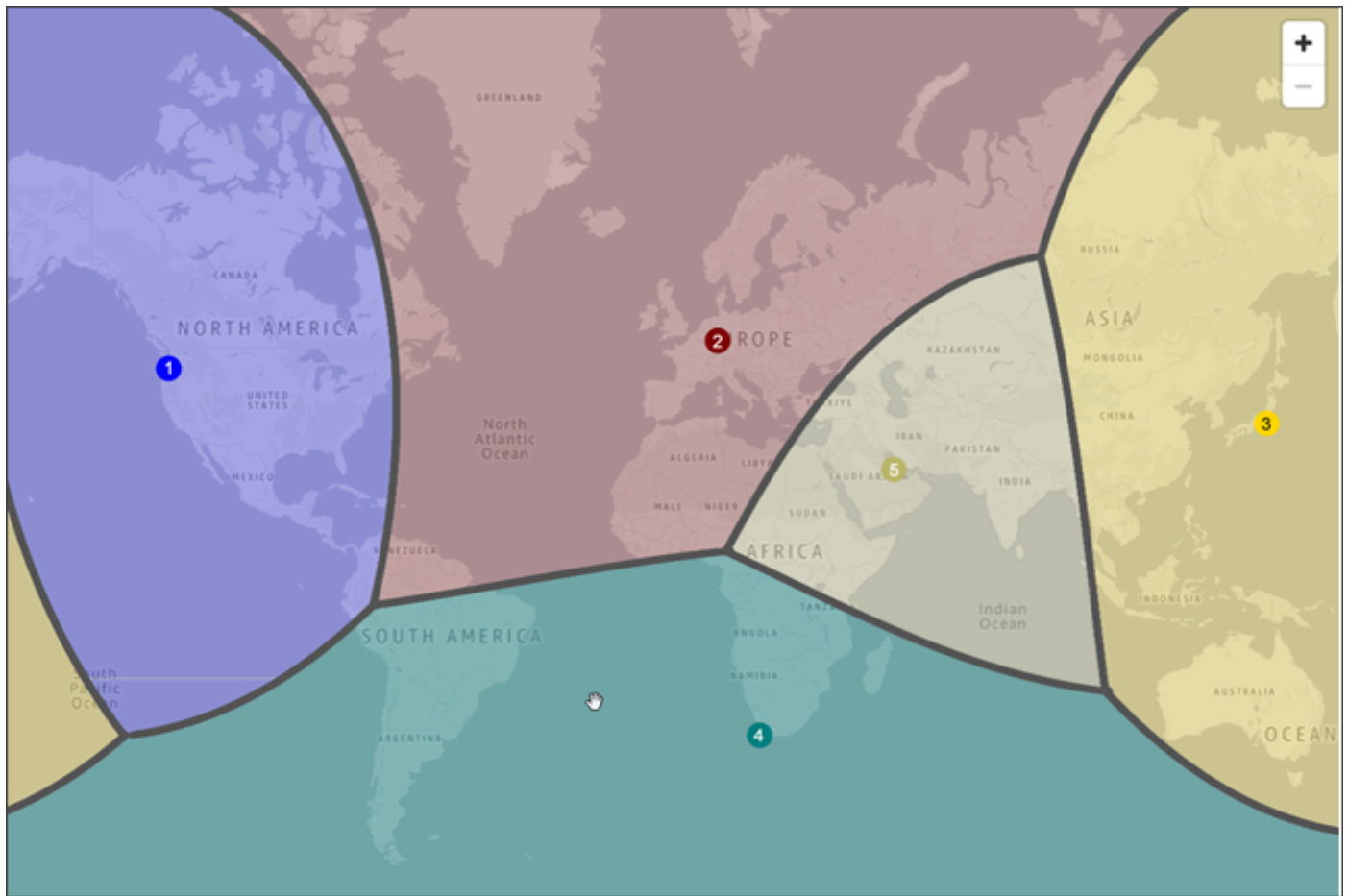
Peta hanya tersedia dengan Arus Lalu Lintas.



Peta berikut menunjukkan apa yang terjadi jika Anda menambahkan bias +25 untuk Wilayah Barat AS (Oregon) (nomor 1 di peta). Lalu lintas diarahkan ke sumber daya di Wilayah itu dari sebagian besar Amerika Utara dan dari seluruh Amerika Selatan daripada sebelumnya.



Peta berikut menunjukkan apa yang terjadi jika Anda mengubah bias menjadi -25 untuk Wilayah Barat AS (Oregon). Lalu lintas dialihkan ke sumber daya di Wilayah itu dari bagian yang lebih kecil di Amerika Utara dan Selatan daripada sebelumnya, dan lebih banyak lalu lintas diarahkan ke sumber daya di wilayah yang berdekatan 2, 3, dan 4.

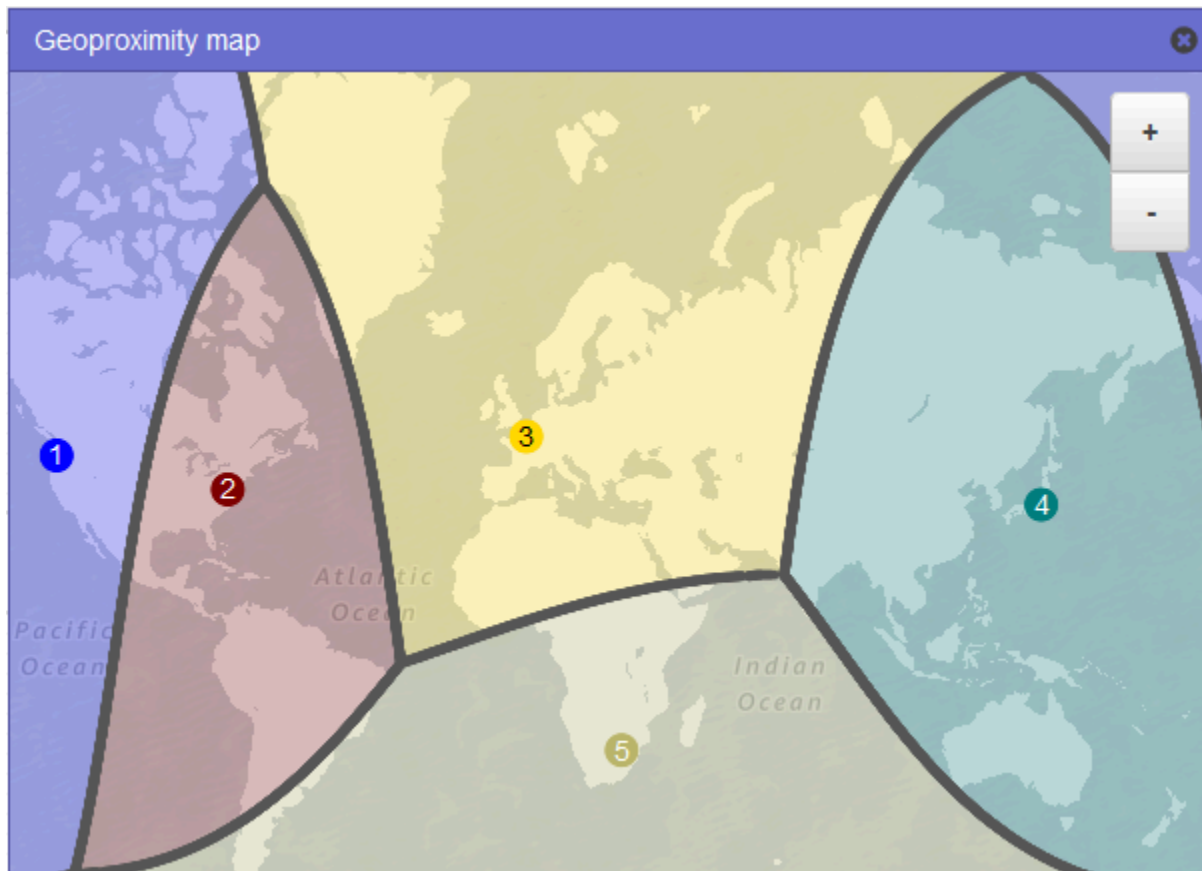


Old console

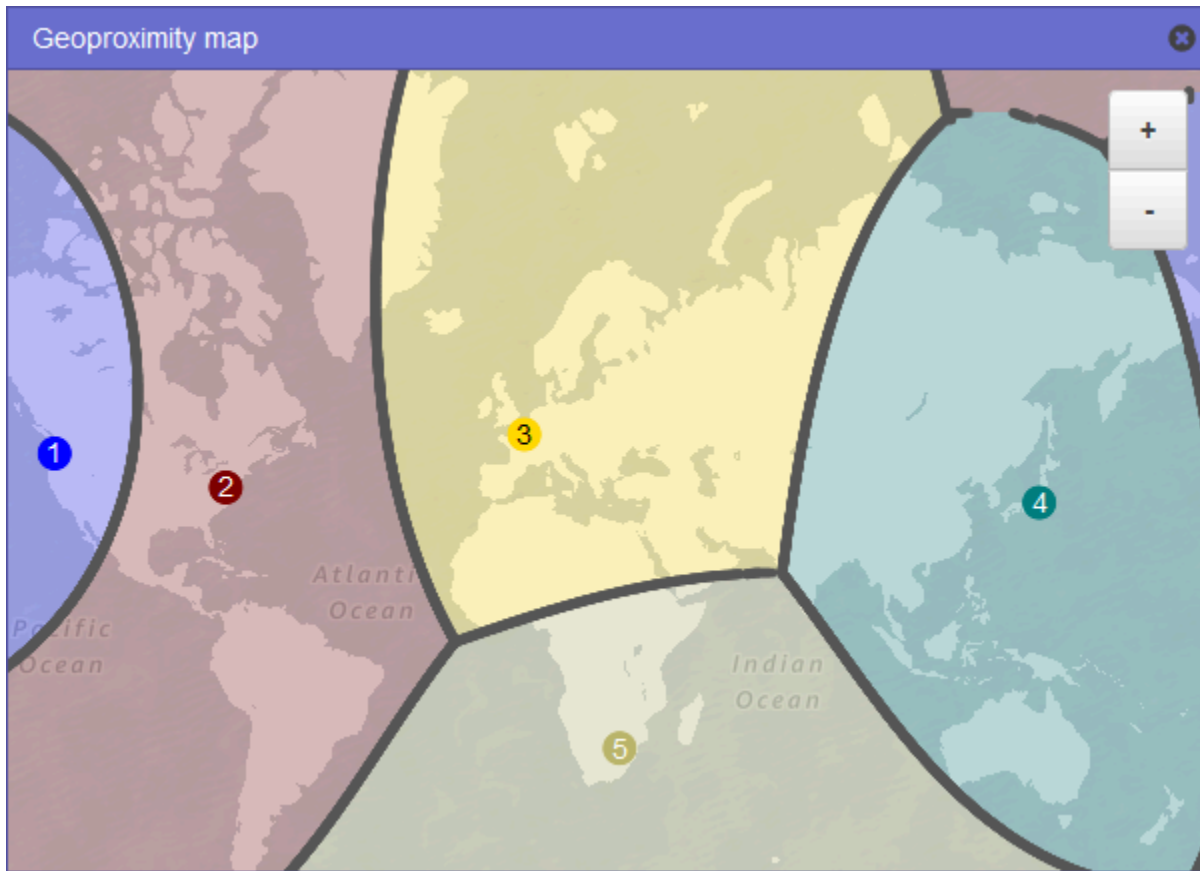
Peta berikut menunjukkan empat Wilayah AWS (nomor 1 sampai 4) dan lokasi di Johannesburg, Afrika Selatan yang ditentukan oleh garis lintang dan bujur (5).

Note

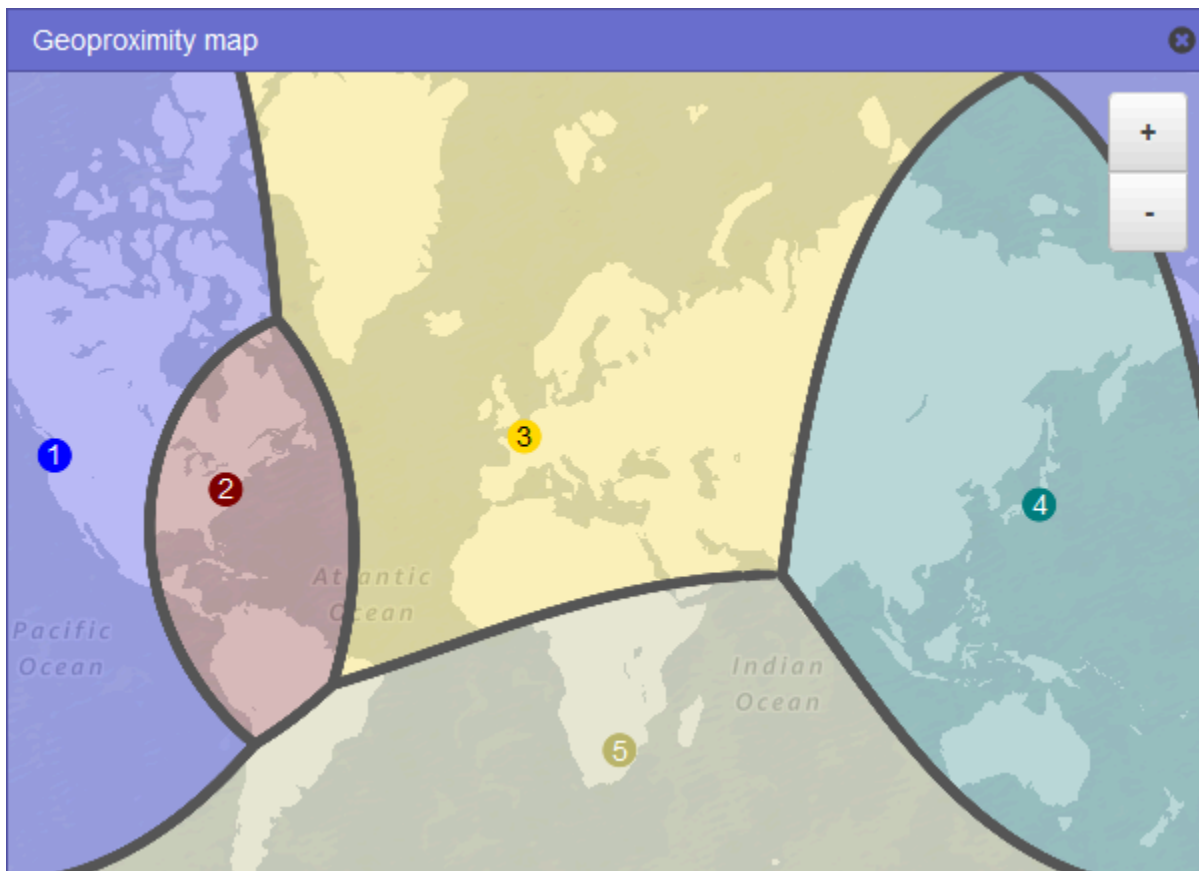
Peta hanya tersedia dengan Arus Lalu Lintas.



Peta berikut menunjukkan apa yang terjadi jika Anda menambahkan bias +25 untuk Wilayah AS Timur (Virginia N.) (nomor 2 di peta). Lalu lintas dialihkan ke sumber daya di Wilayah itu dari sebagian besar Amerika Utara daripada sebelumnya, dan dari seluruh Amerika Selatan.



Peta berikut menunjukkan apa yang terjadi jika Anda mengubah bias menjadi -25 untuk Wilayah AS Timur (Virginia N.). Lalu lintas dirutekan ke sumber daya di Wilayah itu dari bagian yang lebih kecil di Amerika Utara dan Selatan daripada sebelumnya, dan lebih banyak lalu lintas diarahkan ke sumber daya di wilayah yang berdekatan 1, 3, dan 5.



Efek mengubah bias untuk sumber daya Anda bergantung pada sejumlah faktor, termasuk berikut ini:

- Jumlah sumber daya yang Anda miliki.
- Seberapa dekat sumber daya satu sama lain.
- Jumlah pengguna yang Anda miliki di dekat area perbatasan antar wilayah geografis. Misalnya, Anda memiliki sumber daya di Wilayah AWS AS Timur (Virginia N.) dan AS Barat (Oregon), dan Anda memiliki banyak pengguna di Dallas, Austin, dan San Antonio, Texas, AS. Kota-kota itu kira-kira berjarak sama antara sumber daya Anda, sehingga perubahan kecil dalam bias dapat mengakibatkan perubahan besar dalam lalu lintas dari sumber daya satu Wilayah AWS ke yang lain.

Kami menyarankan Anda mengubah bias secara bertahap untuk mencegah sumber daya Anda yang berlebihan, karena perubahan lalu lintas yang tidak terduga.

Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menggunakan EDNS0 untuk memperkirakan lokasi pengguna](#).

Bagaimana Amazon Route 53 menggunakan bias untuk merutekan lalu lintas

Berikut rumus yang digunakan Amazon Route 53 untuk menentukan cara merutekan lalu lintas:

Bias

$$\text{Biased distance} = \text{actual distance} * [1 - (\text{bias}/100)]$$

Ketika nilai bias positif, Route 53 memperlakukan sumber kueri DNS dan sumber daya yang Anda tentukan dalam catatan geoproximity (seperti EC2 instance dalam an Wilayah AWS) seolah-olah mereka lebih dekat daripada yang sebenarnya. Misalnya, anggap Anda memiliki catatan geoproximity berikut:

- Catatan untuk web server A, yang memiliki bias positif 50
- Catatan untuk server web B, yang tidak memiliki bias

Saat catatan geoproximity memiliki bias positif sebesar 50, Route 53 membagi dua jarak antara sumber kueri dan sumber daya untuk rekaman tersebut. Kemudian Route 53 menghitung sumber daya mana yang lebih dekat dengan sumber kueri. Misalkan web server A berjarak 150 kilometer dari sumber kueri dan web server B berjarak 100 kilometer dari sumber kueri. Jika tidak ada catatan yang bias, Route 53 akan merutekan kueri ke server web B karena lebih dekat. Namun, karena catatan untuk server web A memiliki bias positif sebesar 50, Route 53 memperlakukan server web A seolah-olah berjarak 75 kilometer dari sumber kueri. Akibatnya, Route 53 merutekan kueri ke server web A.

Berikut perhitungan untuk bias positif 50:

```
Bias = 50
Biased distance = actual distance * [1 - (bias/100)]

Biased distance = 150 kilometers * [1 - (50/100)]
Biased distance = 150 kilometers * (1 - .50)
Biased distance = 150 kilometers * (.50)
Biased distance = 75 kilometers
```

Perutean berbasis latensi

Jika aplikasi Anda di-host dalam beberapa Wilayah AWS, Anda dapat meningkatkan kinerja untuk pengguna Anda dengan menyajikan permintaan mereka dari Wilayah AWS yang menyediakan latensi terendah.

 Note

Data tentang latensi antara pengguna dan sumber daya Anda didasarkan sepenuhnya pada lalu lintas antara pengguna dan pusat data AWS . Jika Anda tidak menggunakan sumber daya dalam file Wilayah AWS, latensi aktual antara pengguna dan sumber daya Anda dapat sangat bervariasi dari data AWS latensi. Ini benar bahkan jika sumber daya Anda terletak di kota yang sama dengan Wilayah AWS.

Untuk menggunakan perutean berbasis latensi, Anda membuat catatan latensi untuk sumber daya Anda dalam beberapa Wilayah AWS. Saat Route 53 menerima kueri DNS untuk domain atau subdomain Anda (example.com atau acme.example.com), Route 53 menentukan untuk mana Wilayah AWS Anda telah membuat catatan latensi, menentukan Wilayah mana yang memberikan latensi terendah kepada pengguna, dan kemudian memilih catatan latensi untuk Wilayah tersebut. Route 53 merespons dengan nilai dari catatan yang dipilih, seperti alamat IP untuk server web.

Misalnya, Anda memiliki penyeimbang beban Elastic Load Balancing di Wilayah AS Barat (Oregon) dan di Wilayah Asia Pasifik (Singapura). Anda membuat catatan latensi untuk setiap penyeimbang beban. Inilah yang terjadi saat pengguna di London memasukkan nama domain Anda di peramban:

1. DNS merutekan kueri ke server nama Route 53.
2. Route 53 mengacu pada datanya tentang latensi antara London dan Wilayah Singapura dan antara London dan Wilayah Oregon.
3. Jika latensi lebih rendah antara Wilayah London dan Oregon, Route 53 merespons kueri dengan alamat IP untuk penyeimbang beban Oregon. Jika latensi lebih rendah antara London dan Wilayah Singapura, Route 53 merespons dengan alamat IP untuk penyeimbang beban Singapura.

Latensi antara host di internet dapat berubah seiring waktu sebagai akibat dari perubahan konektivitas jaringan dan perutean. Perutean berbasis latensi didasarkan pada pengukuran latensi yang dilakukan selama periode waktu tertentu, dan pengukuran mencerminkan perubahan ini. Permintaan yang dialihkan ke Wilayah Oregon minggu ini mungkin akan dialihkan ke Wilayah Singapura minggu depan.

 Note

Ketika browser atau penampil lain menggunakan DNS resolver yang mendukung edns-client-subnet ekstensi EDNS0, DNS resolver mengirimkan Route 53 versi terpotong

dari alamat IP pengguna. Jika Anda mengonfigurasi perutean berbasis latensi, Route 53 mempertimbangkan nilai ini saat merutekan lalu lintas ke sumber daya Anda. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menggunakan EDNS0 untuk memperkirakan lokasi pengguna](#).

Anda dapat menggunakan kebijakan perutean latensi untuk catatan di zona host pribadi.

Untuk informasi tentang nilai yang Anda tentukan saat menggunakan kebijakan perutean latensi untuk membuat catatan, lihat topik berikut ini:

- [Nilai khusus untuk catatan latensi](#)
- [Nilai khusus untuk catatan alias latensi](#)
- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Perutean berbasis latensi di zona host pribadi

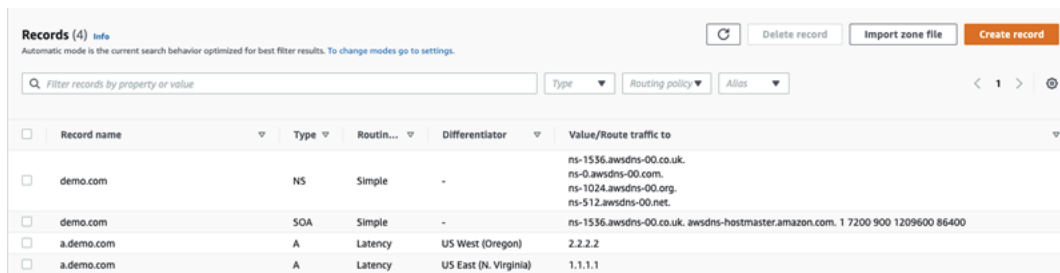
Untuk zona yang dihosting pribadi, Route 53 menjawab kueri DNS dengan titik akhir yang sama Wilayah AWS, atau jaraknya paling dekat dengan VPC Wilayah AWS tempat kueri berasal.

Note

Jika Anda memiliki titik akhir keluar yang diteruskan ke titik akhir masuk, catatan akan diselesaikan berdasarkan di mana titik akhir masuk berada, bukan titik akhir keluar.

Jika Anda menyertakan pemeriksaan kesehatan, dan catatan dengan latensi terendah ke asal kueri tidak sehat, titik akhir yang sehat dengan latensi terendah berikutnya akan dikembalikan.

Dalam konfigurasi contoh pada gambar berikut, kueri DNS yang berasal dari us-east-1, atau yang paling dekat dengannya Wilayah AWS, akan dirutekan ke titik akhir 1.1.1.1. Kueri DNS dari us-west-2, atau yang paling dekat dengannya, akan dirutekan ke titik akhir 2.2.2.2.



Record name	Type	Routing policy	Differentiator	Value/Route traffic to
demo.com	NS	Simple	-	ns-1536.awdns-00.co.uk, ns-0.awdns-00.com, ns-1024.awdns-00.org, ns-512.awdns-00.net
demo.com	SOA	Simple	-	ns-1536.awdns-00.co.uk, awdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
a.demo.com	A	Latency	US West (Oregon)	2.2.2.2
a.demo.com	A	Latency	US East (N. Virginia)	1.1.1.1

Perutean berbasis IP

Dengan perutean berbasis IP di Amazon Route 53, Anda dapat menyempurnakan perutean DNS Anda dengan menggunakan pemahaman Anda tentang jaringan, aplikasi, dan klien Anda untuk membuat keputusan perutean DNS terbaik bagi pengguna akhir Anda. Perutean berbasis IP memberi Anda kontrol granular untuk mengoptimalkan kinerja atau mengurangi biaya jaringan dengan mengunggah data Anda ke Route 53 dalam bentuk pemetaan. user-IP-to-endpoint

Perutean berbasis geolokasi dan latensi didasarkan pada data yang dikumpulkan dan diperbarui oleh Route 53. Pendekatan ini bekerja dengan baik untuk sebagian besar pelanggan, tetapi perutean berbasis IP menawarkan Anda kemampuan tambahan untuk mengoptimalkan perutean berdasarkan pengetahuan khusus tentang basis pelanggan Anda. Misalnya, penyedia konten video global mungkin ingin merutekan pengguna akhir dari penyedia layanan internet (ISP) tertentu.

Beberapa kasus penggunaan umum untuk perutean berbasis IP adalah sebagai berikut:

- Anda ingin merutekan pengguna akhir dari titik akhir tertentu ISPs ke titik akhir tertentu sehingga Anda dapat mengoptimalkan biaya atau kinerja transit jaringan.
- Anda ingin menambahkan penggantian ke jenis perutean Route 53 yang ada, seperti perutean geolokasi, berdasarkan pengetahuan Anda tentang lokasi fisik klien Anda.

Mengelola rentang IP dan mengaitkannya ke kumpulan catatan sumber daya () RRSets

Untuk IPv4, Anda dapat menggunakan blok CIDR dengan panjang antara 1 dan 24 bit, inklusif, sedangkan untuk IPv6, Anda dapat menggunakan blok CIDR dengan panjang antara 1 dan 48 bit, inklusif. Untuk menentukan blok CIDR nol bit (0.0.0.0/0 atau ::/0), gunakan lokasi default ("*").

Untuk kueri DNS dengan CIDR yang lebih panjang dari yang ditentukan dalam koleksi CIDR, Route 53 akan mencocokkannya dengan CIDR yang lebih pendek. Misalnya, jika Anda menentukan 2001:0DB8::/32 sebagai blok CIDR dalam koleksi CIDR Anda dan kueri berasal dari 2001:0DB8:0000:1234::/48, itu akan cocok. Jika, di sisi lain, Anda menentukan 2001:0DB8:0000:1234::/48

dalam koleksi CIDR Anda dan kueri berasal dari 2001:0DB8:::/32, ini tidak akan cocok dan Route 53 akan menjawab dengan catatan untuk lokasi default (“*”).

Anda dapat mengelompokkan kumpulan blok CIDR (atau rentang IP) ke dalam lokasi CIDR, yang pada gilirannya dikelompokkan ke dalam entitas yang dapat digunakan kembali yang disebut koleksi CIDR:

Blok CIDR

Rentang IP dalam notasi CIDR, misalnya, 192.0.2.0/24 atau 2001:::/32. DB8

Lokasi CIDR

Daftar bernama blok CIDR. Misalnya, `example-isp-seattle` = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001:::/32]. DB8 Blok dalam daftar lokasi CIDR tidak harus berdekatan atau rentang yang sama.

Satu lokasi dapat memiliki keduanya IPv4 dan IPv6 blok, dan lokasi ini dapat dikaitkan dengan set rekor A dan AAAA, masing-masing.

Nama lokasi sering merupakan lokasi berdasarkan konvensi, tetapi dapat berupa string apa pun, misalnya, `Perusahaan-A`.

Koleksi CIDR

Koleksi lokasi bernama. Misalnya, `mycollection` = [`example-isp-seattle`, `example-isp-tokyo`].

Set catatan sumber daya perutean berbasis IP mereferensikan lokasi dalam sebuah koleksi, dan semua set catatan sumber daya untuk nama dan tipe set catatan yang sama harus mereferensikan koleksi yang sama. Misalnya, jika Anda membuat situs web di dua Wilayah dan ingin mengarahkan kueri DNS dari dua lokasi CIDR yang berbeda ke situs web tertentu berdasarkan alamat IP asal, maka kedua lokasi tersebut harus terdaftar dalam koleksi CIDR yang sama.

Anda tidak dapat menggunakan kebijakan perutean berbasis IP untuk catatan di zona host pribadi.

Untuk informasi tentang nilai yang Anda tentukan saat menggunakan kebijakan perutean berbasis IP untuk membuat catatan, lihat topik berikut:

- [Nilai khusus untuk catatan berbasis IP](#)
- [Nilai khusus untuk catatan alias berbasis IP](#)

- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Topik

- [Membuat koleksi CIDR dengan lokasi dan blok CIDR](#)
- [Bekerja dengan lokasi dan blok CIDR](#)
- [Menghapus koleksi CIDR](#)
- [Memindahkan geolokasi ke perutean berbasis IP](#)

Membuat koleksi CIDR dengan lokasi dan blok CIDR

Untuk memulai, buat koleksi CIDR dan tambahkan blok dan lokasi CIDR ke dalamnya.

Untuk membuat koleksi CIDR menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih perutean berbasis IP, lalu koleksi CIDR.
3. Pilih Buat koleksi CIDR.
4. Di panel Buat koleksi CIDR, di bawah Detail, masukkan nama untuk koleksi.
5. Pilih Buat koleksi untuk membuat koleksi kosong.

- atau -

Di bagian Buat lokasi CIDR, masukkan nama untuk lokasi CIDR di kotak lokasi CIDR. Nama lokasi dapat berupa string pengidentifikasi, misalnya **company 1**, atau **Seattle**. Tidak harus menjadi lokasi geografis yang sebenarnya.

Important

Nama lokasi CIDR memiliki panjang maksimum 16 karakter.

Masukkan blok CIDR di kotak blok CIDR satu per baris. Ini bisa berupa IPv4 atau IPv6 alamat mulai dari /0 hingga /24 untuk IPv4 dan /0 hingga /48 untuk IPv6

6. Setelah Anda memasukkan blok CIDR, pilih Buat koleksi CIDR, atau Tambahkan lokasi lain untuk tetap memasukkan lokasi dan blok CIDR. Anda dapat memasukkan beberapa lokasi CIDR per koleksi.
7. Setelah Anda memasukkan lokasi CIDR, pilih Buat koleksi CIDR.

Bekerja dengan lokasi dan blok CIDR

Untuk bekerja dengan lokasi CIDR dengan menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih perutean berbasis IP, koleksi CIDR dan kemudian, di bagian koleksi CIDR, klik tautan ke koleksi CIDR di daftar nama Koleksi.

Pada halaman lokasi CIDR, Anda dapat membuat lokasi CIDR, menghapusnya, atau mengedit lokasi dan bloknnya.

- Untuk membuat lokasi, pilih Buat lokasi CIDR.
- Di panel Buat lokasi CIDR, masukkan nama untuk lokasi, blok CIDR yang terkait dengan lokasi, lalu pilih Buat.
- Untuk melihat lokasi CIDR dan blok di dalamnya, pilih tombol radio di sebelah lokasi untuk menampilkan nama dan blok CIDR di panel lokasi.

Di panel ini, Anda juga dapat memilih Edit untuk memperbarui nama lokasi atau blok CIDR-nya. Pilih Simpan setelah Anda selesai mengedit.

- Untuk menghapus lokasi CIDR dan blok di dalamnya, pilih tombol radio di sebelah lokasi yang ingin Anda hapus, lalu pilih Hapus. Untuk mengonfirmasi penghapusan, masukkan nama lokasi di bidang input teks dan pilih Hapus lagi.

Important

Menghapus lokasi CIDR tidak dapat dibatalkan. Jika Anda memiliki catatan DNS yang terkait dengan lokasi, domain Anda mungkin tidak dapat dijangkau.

Menghapus koleksi CIDR

Untuk menghapus koleksi CIDR, lokasinya, dan bloknnya dengan menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih perutean berbasis IP dan kemudian koleksi CIDR.
3. Di bagian koleksi CIDR, klik nama yang ditautkan dari koleksi yang ingin Anda hapus.
4. Pada halaman lokasi CIDR, pilih setiap lokasi satu per satu, pilih Hapus, masukkan namanya di kotak dialog, lalu pilih Hapus. Anda harus menghapus setiap lokasi yang terkait dengan koleksi CIDR sebelum Anda dapat menghapus koleksi.
5. Setelah penghapusan setiap lokasi CIDR selesai, pada halaman lokasi CIDR, pilih tombol radio di sebelah koleksi yang ingin Anda hapus, lalu pilih Hapus.

Memindahkan geolokasi ke perutean berbasis IP

Jika Anda menggunakan kebijakan perutean geolokasi atau geoproximity, dan Anda secara konsisten melihat klien tertentu dirutekan ke titik akhir yang tidak optimal berdasarkan lokasi fisik atau topologi jaringan mereka, Anda dapat menargetkan rentang IP publik klien ini dengan lebih baik dengan menggunakan IP berbasis routing.

Tabel berikut berisi contoh konfigurasi geolokasi untuk perutean geolokasi yang ada yang akan kami sempurnakan untuk rentang IP California.

Rekam nama set	Kebijakan dan asal perutean	Alamat IP dari titik akhir aplikasi
contoh.com	Geolokasi-routing (AS)	198.51.100.1
contoh.com	Perutean geolokasi (UE)	198.51.100.2

Untuk mengganti rentang IP dari California untuk pergi ke titik akhir aplikasi baru, pertama-tama buat ulang perutean geolokasi di bawah nama set catatan baru.

Rekam nama set	Kebijakan dan asal perutean	Alamat IP dari titik akhir aplikasi

Rekam nama set	Kebijakan dan asal perutean	Alamat IP dari titik akhir aplikasi
geo.example.com	Geolokasi-routing (AS)	198.51.100.1
geo.example.com	Perutean geolokasi (UE)	198.51.100.2

Kemudian, buat catatan perutean berbasis IP dan catatan default yang menunjuk ke kumpulan rekaman perutean geolokasi yang baru saja dibuat ulang.

Rekam nama set	Kebijakan dan asal perutean	Alamat IP dari titik akhir aplikasi
contoh.com	Perutean berbasis IP (default)	Alias merekam ke titik akhir aplikasi geo.example.com yang ingin Anda jadikan default. Misalnya, 198.51.100.1 .
contoh.com	Perutean berbasis IP (rentang IP California)	198.51.100.3

Perutean jawaban multinilai

Perutean jawaban multinilai memungkinkan Anda mengonfigurasi Amazon Route 53 untuk mengembalikan beberapa nilai, seperti alamat IP untuk server web Anda, sebagai respons terhadap kueri DNS. Anda dapat menentukan beberapa nilai untuk hampir semua catatan, tetapi perutean jawaban multinilai juga memungkinkan Anda memeriksa kondisi setiap sumber daya, jadi Route 53 hanya mengembalikan nilai untuk sumber daya yang sehat. Ini bukan pengganti penyeimbang beban, tetapi kemampuan untuk mengembalikan beberapa alamat IP yang dapat diperiksa kondisinya adalah cara menggunakan DNS untuk meningkatkan ketersediaan dan penyeimbangan beban.

Untuk merutekan lalu lintas secara kira-kira secara acak ke beberapa sumber daya, seperti server web, Anda membuat satu catatan jawaban multinilai untuk setiap sumber daya dan, secara opsional, mengaitkan pemeriksaan kondisi Route 53 dengan setiap catatan. Route 53 merespons kueri DNS

dengan hingga delapan catatan yang sehat dan memberikan jawaban yang berbeda untuk DNS resolver yang berbeda. Jika server web menjadi tidak tersedia setelah resolver men-cache respons, perangkat lunak klien dapat mencoba alamat IP lain dalam respons.

Perhatikan hal-hal berikut:

- Jika Anda mengaitkan pemeriksaan kondisi dengan catatan jawaban multivalai, Route 53 merespons kueri DNS dengan alamat IP yang sesuai hanya saat pemeriksaan kondisi yang baik.
- Jika Anda tidak mengaitkan pemeriksaan kondisi dengan catatan jawaban multivalai, Route 53 selalu menganggap catatan tersebut sehat.
- Jika Anda memiliki delapan catatan kondisi baik atau kurang dari itu, maka Route 53 menanggapi semua kueri DNS dengan semua catatan kondisi baik.
- Saat semua catatan tidak sehat, Route 53 akan merespons kueri DNS dengan hingga delapan catatan yang tidak sehat.

Anda dapat menggunakan kebijakan perutean jawaban multivalue untuk catatan di zona host pribadi.

Untuk informasi tentang nilai yang Anda tentukan saat Anda menggunakan kebijakan perutean jawaban multivalue untuk membuat catatan, lihat dan. [Nilai khusus untuk catatan jawaban multivalue](#)
[Nilai yang umum untuk semua kebijakan perutean](#)

Perutean tertimbang

Perutean tertimbang memungkinkan Anda mengaitkan beberapa sumber daya dengan satu nama domain (example.com) atau nama subdomain (acme.example.com) dan memilih berapa banyak lalu lintas yang diarahkan ke setiap sumber daya. Ini dapat berguna untuk berbagai tujuan, termasuk penyeimbangan beban dan pengujian perangkat lunak versi baru.

Untuk mengonfigurasi perutean berbobot, Anda membuat catatan yang memiliki nama dan jenis yang sama untuk setiap sumber daya Anda. Anda menetapkan setiap catatan bobot relatif yang sesuai dengan berapa banyak lalu lintas yang ingin Anda kirim ke setiap sumber daya. Amazon Route 53 mengirimkan lalu lintas ke sumber daya berdasarkan bobot yang Anda tetapkan ke catatan sebagai proporsi dari total bobot untuk semua catatan dalam grup:

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

Misalnya, jika Anda ingin mengirim sebagian kecil lalu lintas ke satu sumber daya dan sisanya ke sumber daya lain, Anda dapat menentukan bobot 1 dan 255. Sumber daya dengan bobot 1

mendapat $1/256$ lalu lintas ($1/(1+255)$), dan sumber daya lainnya mendapat $255/256$ ($255/(1+255)$). Anda dapat secara bertahap mengubah keseimbangan dengan mengubah bobot. Jika Anda ingin berhenti mengirim lalu lintas ke sumber daya, Anda dapat mengubah berat untuk catatan tersebut ke 0.

Untuk informasi tentang nilai yang Anda tentukan saat menggunakan kebijakan perutean berbobot untuk membuat catatan, lihat topik berikut ini:

- [Nilai khusus untuk catatan tertimbang](#)
- [Nilai khusus untuk catatan alias tertimbang](#)
- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Anda dapat menggunakan kebijakan perutean tertimbang untuk catatan di zona host pribadi.

Pemeriksaan kesehatan dan perutean tertimbang

Jika Anda menambahkan pemeriksaan kondisi ke semua catatan dalam grup catatan tertimbang, tetapi Anda memberikan bobot non-nol ke beberapa catatan dan bobot nol untuk catatan lainnya, pemeriksaan kondisi bekerja seperti ketika semua catatan memiliki bobot non-nol dengan pengecualian berikut:

- Route 53 awalnya hanya mempertimbangkan catatan tertimbang non-nol, jika ada.
- Jika semua catatan yang memiliki bobot lebih besar dari 0 dalam kondisi tidak sehat, Route 53 mempertimbangkan catatan tertimbang nol.

Tabel berikut merinci perilaku ketika catatan 0-berat mencakup pemeriksaan kesehatan:

	Rekam 1	Rekam 2	Rekam 3
Bobot	1	1	0
Termasuk pemeriksaan kesehatan?	Ya	Ya	Ya

	Rekam 1	Rekam 2	Rekam 3
Status pemeriksaan kondisi	Tidak sehat	Tidak sehat	Sehat
Kueri DNS dijawab?	Tidak	Tidak	Ya
Status pemeriksaan kondisi	Tidak sehat	Tidak sehat	Tidak sehat
Kueri DNS dijawab?	Ya	Ya	Tidak
Status pemeriksaan kondisi	Tidak sehat	Sehat	Tidak sehat
Kueri DNS dijawab?	Tidak	Ya	Tidak
Status pemeriksaan kondisi	Sehat	Sehat	Tidak sehat
Kueri DNS dijawab?	Ya	Ya	Tidak
Status pemeriksaan kondisi	Sehat	Sehat	Sehat
Kueri DNS dijawab?	Ya	Ya	Tidak

Tabel berikut merinci perilaku ketika catatan 0-berat tidak termasuk pemeriksaan kesehatan:

Rekam 1	Rekam 2	Rekam 3

	Rekam 1	Rekam 2	Rekam 3
Bobot	1	1	0
Termasuk pemeriksaan kesehatan?	Ya	Ya	Tidak
Status pemeriksaan kondisi	Sehat	Sehat	N/A
Kueri DNS dijawab?	Ya	Ya	Tidak
Status pemeriksaan kondisi	Tidak sehat	Tidak sehat	N/A
Kueri DNS dijawab?	Tidak	Tidak	Ya
Status pemeriksaan kondisi	Tidak sehat	Sehat	N/A
Kueri DNS dijawab?	Tidak	Ya	Tidak

Bagaimana Amazon Route 53 menggunakan EDNS0 untuk memperkirakan lokasi pengguna

Untuk meningkatkan akurasi perutean geolokasi, geoproximity, berbasis IP, dan latensi, Amazon Route 53 mendukung perpanjangan EDNS0. `edns-client-subnet` (EDNS0 menambahkan beberapa ekstensi opsional ke protokol DNS.) Route 53 `edns-client-subnet` hanya dapat digunakan ketika resolver DNS mendukungnya:

- Ketika browser atau penampil lain menggunakan resolver DNS yang tidak mendukung edns-client-subnet, Route 53 menggunakan alamat IP sumber dari DNS resolver untuk memperkirakan lokasi pengguna dan merespons kueri geolokasi dengan catatan DNS untuk lokasi resolver.
- Ketika browser atau penampil lain menggunakan DNS resolver yang mendukung edns-client-subnet, DNS resolver mengirimkan Route 53 versi terpotong dari alamat IP pengguna. Route 53 menentukan lokasi pengguna berdasarkan alamat IP yang terpotong daripada alamat IP sumber dari DNS resolver; ini biasanya memberikan perkiraan lokasi pengguna yang lebih akurat. Route 53 kemudian merespons kueri geolokasi dengan catatan DNS untuk lokasi pengguna.
- EDNS0 tidak berlaku untuk zona host pribadi. Untuk zona yang dihosting pribadi, Route 53 menggunakan data dari Resolver VPC di tempat zona host pribadi berada untuk membuat keputusan perutean geolokasi dan latensi. Wilayah AWS

Untuk informasi selengkapnya edns-client-subnet, lihat EDNS Client Subnet RFC, Client Subnet in DNS [Requests](#).

Memilih antara catatan alias dan nonalias

Catatan alias Amazon Route 53 menyediakan ekstensi khusus Route 53 untuk fungsionalitas DNS. Catatan alias memungkinkan Anda merutekan lalu lintas ke AWS sumber daya yang dipilih, termasuk namun tidak terbatas pada, CloudFront distribusi, dan bucket Amazon S3. Mereka juga memungkinkan Anda merutekan lalu lintas dari satu catatan di zona yang di-hosting ke catatan lain.

Tidak seperti catatan CNAME, Anda dapat membuat catatan alias di node atas dari namespace DNS, yang juga dikenal sebagai zone apex. Misalnya, jika Anda mendaftarkan nama DNS `example.com`, zone apex-nya adalah `example.com`. Anda tidak dapat membuat catatan CNAME untuk `example.com`, tetapi Anda dapat membuat catatan alias untuk `example.com` yang merutekan lalu lintas ke `www.example.com` (selama jenis rekaman untuk `www.example.com` bukan tipe CNAME).

Saat Route 53 menerima kueri DNS untuk catatan alias, Route 53 merespons dengan nilai yang berlaku untuk sumber daya tersebut:

- API regional kustom Amazon API Gateway atau API yang dioptimalkan edge – Route 53 merespons dengan satu atau lebih alamat IP untuk API Anda.
- Titik akhir antarmuka Amazon VPC – Route 53 merespons dengan satu atau lebih alamat IP untuk titik akhir antarmuka Anda.

- CloudFront Distribusi — Route 53 merespons dengan satu atau lebih alamat IP untuk server CloudFront edge yang dapat melayani konten Anda.
- Layanan Pelari Aplikasi - Route 53 merespons dengan satu atau lebih alamat IP.
- Lingkungan Elastic Beanstalk— Route 53 merespons dengan satu atau lebih alamat IP untuk lingkungan.
- Penyeimbang beban Elastic Load Balancing — Route 53 merespons dengan satu atau lebih alamat IP untuk penyeimbang beban. Ini termasuk Application Load Balancer, Classic Load Balancer dan, Network Load Balancer.
- AWS Global Accelerator Akselerator — Route 53 merespons dengan alamat IP untuk akselerator.
- OpenSearch Layanan — Route 53 merespons dengan satu atau beberapa alamat IP untuk domain kustom OpenSearch Layanan.
- Bucket Amazon S3 yang dikonfigurasi sebagai situs web statis- Route 53 merespons dengan satu alamat IP untuk bucket Amazon S3.
- Catatan Route 53 lainnya dari jenis yang sama di zona host yang sama — Route 53 merespons seolah-olah kueri adalah untuk catatan yang direferensikan oleh catatan alias (lihat). [Perbandingan catatan alias dan CNAME](#)
- AWS AppSync nama domain — Route 53 merespons dengan satu atau lebih alamat IP untuk titik akhir antarmuka Anda.

Untuk informasi selengkapnya, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Saat Anda menggunakan catatan alias untuk merutekan lalu lintas ke AWS sumber daya, Route 53 secara otomatis mengenali perubahan dalam sumber daya. Misalnya, catatan alias untuk example.com menunjuk ke penyeimbang beban Elastic Load Balancing di lb1-1234.us-east-2.elb.amazonaws.com. Jika alamat IP penyeimbang beban berubah, Route 53 secara otomatis mulai merespons permintaan DNS menggunakan alamat IP baru.

Jika catatan alias menunjuk ke AWS sumber daya, Anda tidak dapat mengatur waktu untuk hidup (TTL); Route 53 menggunakan TTL default untuk sumber daya. Jika catatan alias menunjuk ke catatan lain di zona yang di-hosting yang sama, Route 53 menggunakan TTL catatan yang ditunjuk oleh catatan alias. Untuk informasi lebih lanjut tentang nilai TTL saat ini untuk Elastic Load Balancing, buka [Meminta perutean](#) di Panduan Pengguna Elastic Load Balancing dan cari "ttl".

Untuk informasi tentang membuat catatan menggunakan konsol Route 53, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#). Untuk informasi tentang nilai yang Anda tentukan

untuk catatan alias, lihat topik yang berlaku di [Nilai yang Anda tentukan saat membuat atau mengedit catatan Amazon Route 53](#):

- [Nilai khusus untuk catatan alias sederhana](#)
- [Nilai khusus untuk catatan alias tertimbang](#)
- [Nilai khusus untuk catatan alias latensi](#)
- [Nilai khusus untuk catatan alias failover](#)
- [Nilai khusus untuk catatan alias geolokasi](#)
- [Nilai khusus untuk catatan alias geoproximity](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

Perbandingan catatan alias dan CNAME

Catatan alias mirip dengan catatan CNAME, tetapi ada beberapa perbedaan penting. Daftar berikut membandingkan data alias dan data CNAME.

Sumber daya tempat Anda dapat mengarahkan kueri

Catatan Alias

Catatan alias hanya dapat mengarahkan kueri ke AWS sumber daya yang dipilih, termasuk namun tidak terbatas pada hal berikut:

- Bucket Amazon S3
- CloudFront distribusi
- Catatan lain dalam zona yang di-hosting Route 53 yang sama

Misalnya, Anda dapat membuat catatan alias bernama `acme.example.com` yang mengalihkan kueri ke bucket Amazon S3 yang juga bernama `acme.example.com`. Anda juga dapat membuat catatan alias `acme.example.com` yang mengalihkan kueri ke catatan bernama `zenith.example.com` di zona yang di-hosting `example.com`.

Catatan CNAME

Data CNAME dapat mengalihkan kueri DNS ke data DNS apa pun. Misalnya, Anda dapat membuat data CNAME yang mengalihkan kueri dari `acme.example.com` ke `zenith.example.com` atau ke `acme.example.org`. Anda tidak perlu menggunakan Route 53 sebagai layanan DNS untuk domain tujuan pengalihan kueri.

Membuat catatan yang memiliki nama yang sama dengan domain (catatan di zone apex)

Catatan Alias

Di sebagian besar konfigurasi, Anda dapat membuat catatan alias yang memiliki nama yang sama dengan zona yang di-hosting (zone apex). Satu-satunya pengecualian adalah ketika Anda ingin mengalihkan kueri dari zone apex (seperti example.com) ke catatan di zona yang di-hosting yang sama yang memiliki tipe CNAME (seperti zenith.example.com). Catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Catatan CNAME

Anda tidak dapat membuat data CNAME yang memiliki nama yang sama dengan zona yang di-hosting (zone apex). Hal ini berlaku baik untuk zona yang di-hosting untuk nama domain (example.com) dan untuk zona yang di-hosting untuk subdomain (zenith.example.com).

Harga untuk kueri DNS

Catatan alias

Route 53 tidak mengenakan biaya untuk kueri alias ke AWS sumber daya. Untuk informasi lebih lanjut, lihat [Harga Amazon Route 53](#).

Catatan CNAME

Route 53 biaya untuk kueri CNAME.

Note

Jika Anda membuat catatan CNAME yang mengalihkan ke nama catatan lain di zona yang di-hosting Route 53 (zona yang di-hosting yang sama atau zona yang di-hosting lain), setiap kueri DNS dibebankan sebagai dua kueri:

- Route 53 merespons kueri DNS pertama dengan nama catatan yang ingin Anda alihkan.
- Kemudian DNS resolver harus mengirimkan kueri lain untuk dicatat dalam respons pertama untuk mendapatkan informasi tentang ke mana merutekan lalu lintas, misalnya, alamat IP server web.

Jika data CNAME dialihkan ke nama data yang di-hosting dengan layanan DNS lain, Route 53 mengenakan biaya untuk satu kueri. Layanan DNS lainnya mungkin mengenakan biaya untuk kueri kedua.

Jenis catatan yang ditentukan dalam kueri DNS

Catatan Alias

Route 53 merespons kueri DNS hanya jika nama catatan alias (seperti `acme.example.com`) dan jenis catatan alias (seperti `A` atau `AAAA`) cocok dengan nama dan ketik kueri DNS.

Catatan CNAME

Data CNAME mengalihkan kueri DNS untuk nama catatan terlepas dari jenis catatan yang ditentukan dalam kueri DNS, seperti `A` atau `AAAA`.

Cara catatan dicantumkan dalam kueri pencarian atau nslookup

Catatan Alias

Dalam respons terhadap kueri pencarian atau nslookup, catatan alias dicantumkan sebagai tipe catatan yang Anda tentukan saat Anda membuat catatan, seperti `A` atau `AAAA`. (Jenis catatan yang Anda tentukan untuk catatan alias bergantung pada sumber daya tujuan rute lalu lintas Anda. Misalnya, untuk merutekan lalu lintas ke bucket S3, Anda menentukan `A` untuk jenisnya.) Properti alias hanya terlihat di konsol Route 53 atau sebagai respons terhadap permintaan terprogram, seperti perintah CLI AWS `. list-resource-record-sets`

Catatan CNAME

Catatan CNAME terdaftar sebagai catatan CNAME sebagai tanggapan atas kueri penggalian atau nslookup.

Tipe data DNS yang didukung

Amazon Route 53 mendukung jenis catatan DNS yang tercantum di bagian ini. Setiap jenis catatan juga mencakup contoh bagaimana memformat elemen `Value` ketika Anda mengakses Route 53 menggunakan API.

Note

Untuk jenis catatan yang menyertakan nama domain, masukkan nama domain yang sepenuhnya memenuhi syarat, misalnya, `www.example.com`. Titik akhir adalah opsional; Route 53 mengasumsikan bahwa nama domain sepenuhnya memenuhi syarat. Ini berarti bahwa Route 53 memperlakukan `www.example.com` (tanpa titik akhir) dan `www.example.com.` (dengan titik akhir) sebagai identik.

Route 53 menyediakan ekstensi untuk fungsionalitas DNS yang dikenal sebagai catatan alias. Mirip dengan catatan CNAME, catatan alias memungkinkan Anda merutekan lalu lintas ke AWS sumber daya yang dipilih, seperti CloudFront distribusi dan bucket Amazon S3. Untuk informasi selengkapnya, termasuk perbandingan alias dan data CNAME, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Jenis catatan](#)
- [Jenis catatan AAAA](#)
- [Jenis catatan CAA](#)
- [Jenis catatan CNAME](#)
- [Tipe catatan DS](#)
- [Jenis catatan HTTPS](#)
- [Tipe catatan MX](#)
- [Jenis catatan NAPTR](#)
- [Tipe catatan NS](#)
- [Tipe catatan PTR](#)
- [Jenis catatan SOA](#)
- [Tipe catatan SPF](#)
- [Tipe catatan SRV](#)
- [Jenis catatan SSHFP](#)
- [Jenis catatan SVCB](#)
- [Jenis catatan TLSA](#)
- [Tipe catatan TXT](#)

Jenis catatan

Anda menggunakan catatan A untuk merutekan lalu lintas ke sumber daya, seperti server web, menggunakan IPv4 alamat dalam notasi desimal bertitik.

Contoh untuk konsol Amazon Route 53

```
192.0.2.1
```

Contoh untuk API Route 53

```
<Value>192.0.2.1</Value>
```

Jenis catatan AAAA

Anda menggunakan catatan AAAA untuk merutekan lalu lintas ke sumber daya, seperti server web, menggunakan IPv6 alamat dalam format heksadesimal yang dipisahkan titik dua.

Contoh untuk konsol Amazon Route 53

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Contoh untuk API Route 53

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

Jenis catatan CAA

Catatan CAA menentukan otoritas sertifikat (CAs) mana yang diizinkan untuk mengeluarkan sertifikat untuk domain atau subdomain. Membuat catatan CAA membantu CAs mencegah kesalahan menerbitkan sertifikat untuk domain Anda. Catatan CAA bukanlah pengganti persyaratan keamanan yang ditentukan oleh otoritas sertifikat Anda, seperti persyaratan untuk memvalidasi bahwa Anda adalah pemilik domain.

Anda dapat menggunakan catatan CAA untuk menentukan hal berikut:

- Otoritas sertifikat mana (CAs) yang dapat mengeluarkan SSL/TLS sertifikat, jika ada
- Alamat email atau URL untuk dihubungi saat CA mengeluarkan sertifikat untuk domain atau subdomain

Saat Anda menambahkan catatan CAA ke zona yang di-hosting, Anda menentukan tiga pengaturan yang dipisahkan oleh spasi:

flags tag "value"

Perhatikan hal berikut tentang format untuk catatan CAA:

- Nilai dari tag hanya dapat berisi karakter A-Z, a-z, dan 0-9.
- Selalu lampirkan value dalam tanda petik (").
- Beberapa CAs mengizinkan atau memerlukan nilai tambahan untuk value. Tentukan nilai tambahan sebagai pasangan nama-nilai, dan pisahkan dengan titik koma (;), misalnya:

```
0 issue "ca.example.net; account=123456"
```

- Jika CA menerima permintaan sertifikat untuk subdomain (seperti www.example.com) dan jika tidak ada catatan CAA untuk subdomain, CA mengirimkan permintaan DNS untuk catatan CAA untuk domain induk (seperti example.com). Jika ada catatan untuk domain induk dan jika permintaan sertifikat valid, CA mengeluarkan sertifikat untuk subdomain.
- Kami menyarankan Anda berkonsultasi dengan CA Anda untuk menentukan nilai apa yang harus ditentukan untuk catatan CAA.
- Anda tidak dapat membuat data CAA dan data CNAME yang memiliki nama yang sama karena DNS tidak mengizinkan penggunaan nama yang sama untuk data CNAME dan jenis data lainnya.

Topik

- [Otorisasi CA untuk mengeluarkan sertifikat untuk domain atau subdomain](#)
- [Otorisasi CA untuk mengeluarkan sertifikat wildcard untuk domain atau subdomain](#)
- [Mencegah CA mengeluarkan sertifikat untuk domain atau subdomain](#)
- [Minta agar CA mana pun menghubungi Anda jika CA menerima permintaan sertifikat yang tidak valid](#)
- [Gunakan pengaturan lain yang didukung oleh CA](#)
- [Contoh](#)

Otorisasi CA untuk mengeluarkan sertifikat untuk domain atau subdomain

Untuk mengizinkan CA menerbitkan sertifikat untuk domain atau subdomain, buat catatan yang memiliki nama yang sama dengan domain atau subdomain, dan tentukan pengaturan berikut:

- bendera – 0
- tanda – issue
- nilai – kode untuk CA yang Anda otorisasi untuk mengeluarkan sertifikat untuk domain atau subdomain

Misalnya, Anda ingin mengotorisasi `ca.example.net` untuk mengeluarkan sertifikat untuk `example.com`. Anda membuat catatan CAA untuk `example.com` dengan pengaturan berikut:

```
0 issue "ca.example.net"
```

Untuk informasi tentang cara AWS Certificate Manager mengotorisasi penerbitan sertifikat, lihat [Mengonfigurasi catatan CAA](#) di AWS Certificate Manager Panduan Pengguna.

Otorisasi CA untuk mengeluarkan sertifikat wildcard untuk domain atau subdomain

Untuk mengotorisasi CA untuk mengeluarkan sertifikat wildcard untuk domain atau subdomain, buat catatan yang memiliki nama yang sama dengan domain atau subdomain, dan tentukan pengaturan berikut. Sertifikat wildcard berlaku untuk domain atau subdomain dan semua subdomainnya.

- bendera – 0
- tanda – `issuewild`
- nilai – kode untuk CA yang Anda otorisasi untuk mengeluarkan sertifikat untuk domain atau subdomain, dan subdomainnya

Misalnya, Anda ingin mengotorisasi `ca.example.net` untuk mengeluarkan sertifikat wildcard untuk `example.com`, yang berlaku untuk `example.com` dan semua subdomainnya. Anda membuat catatan CAA untuk `example.com` dengan pengaturan berikut:

```
0 issuewild "ca.example.net"
```

Saat Anda ingin mengotorisasi CA untuk mengeluarkan sertifikat wildcard untuk domain atau subdomain, buat catatan yang memiliki nama yang sama dengan domain atau subdomain, dan tentukan pengaturan berikut. Sertifikat wildcard berlaku untuk domain atau subdomain dan semua subdomainnya.

Mencegah CA mengeluarkan sertifikat untuk domain atau subdomain

Untuk mencegah CA mengeluarkan sertifikat untuk domain atau subdomain, membuat catatan yang memiliki nama yang sama sebagai domain atau subdomain, dan menentukan pengaturan berikut:

- bendera – 0
- tanda – `issue`
- Nilai – `;"`

Misalnya, Anda tidak ingin CA mengeluarkan sertifikat untuk example.com. Anda membuat catatan CAA untuk example.com dengan pengaturan berikut:

```
0 issue ";"
```

Jika Anda tidak ingin CA mengeluarkan sertifikat untuk example.com atau subdomainnya, buat data CAA untuk example.com dengan pengaturan berikut:

```
0 issuewild ";"
```

Note

Jika Anda membuat catatan CAA untuk example.com dan menentukan kedua nilai berikut, CA yang menggunakan nilai ca.example.net dapat mengeluarkan sertifikat untuk example.com:

```
0 issue ";"  
0 issue "ca.example.net"
```

Minta agar CA mana pun menghubungi Anda jika CA menerima permintaan sertifikat yang tidak valid

Jika Anda ingin CA yang menerima permintaan sertifikat yang tidak valid untuk menghubungi Anda, tentukan pengaturan berikut:

- bendera – 0
- tanda – iodef
- nilai – URL atau alamat email yang Anda ingin CA beri tahu jika CA menerima permintaan sertifikat yang tidak valid. Gunakan format yang berlaku:

```
"mailto:email-address"
```

```
"http://URL"
```

```
"https://URL"
```

Misalnya, jika Anda ingin CA yang menerima permintaan sertifikat yang tidak valid untuk mengirim email ke admin@example.com, Anda membuat catatan CAA dengan pengaturan berikut:

```
0 iodef "mailto:admin@example.com"
```

Gunakan pengaturan lain yang didukung oleh CA

Jika CA Anda mendukung fitur yang tidak ditentukan dalam RFC untuk catatan CAA, tentukan pengaturan berikut:

- bendera – 128 (Nilai ini mencegah CA mengeluarkan sertifikat jika CA tidak mendukung fitur yang ditentukan.)
- Tanda— tanda yang Anda otorisasi CA untuk menggunakan
- nilai— nilai yang sesuai dengan nilai tanda

Misalnya, CA Anda mendukung pengiriman pesan teks jika CA menerima permintaan sertifikat yang tidak valid. (Kami tidak mengetahui ada CAs yang mendukung opsi ini.) Pengaturan untuk catatan mungkin sebagai berikut:

```
128 exampletag "15555551212"
```

Contoh

Contoh untuk konsol Route 53

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Contoh untuk API Route 53

```
<ResourceRecord>
  <Value>0 issue "ca.example.net"</Value>
  <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

Jenis catatan CNAME

Data CNAME memetakan kueri DNS untuk nama data saat ini, seperti `acme.example.com`, ke domain lain (`example.com` atau `example.net`) atau subdomain (`acme.example.com` atau `zenith.example.org`).

Important

Protokol DNS tidak mengizinkan Anda membuat catatan CNAME untuk node teratas dari namespace DNS, yang juga dikenal sebagai apex zona. Misalnya, jika Anda mendaftarkan nama DNS `example.com`, zone apex-nya adalah `example.com`. Anda tidak dapat membuat data CNAME untuk `example.com`, tetapi Anda dapat membuat data CNAME untuk `www.example.com`, `newproduct.example.com`, dan seterusnya.

Selain itu, jika Anda membuat data CNAME untuk subdomain, Anda tidak dapat membuat data lain untuk subdomain tersebut. Misalnya, jika Anda membuat CNAME untuk `www.example.com`, Anda tidak dapat membuat catatan lain yang nilai bidang Name-nya adalah `www.example.com`.

Amazon Route 53 juga mendukung catatan alias, yang memungkinkan Anda merutekan kueri ke AWS sumber daya yang dipilih, seperti CloudFront distribusi dan bucket Amazon S3. Alias dalam beberapa hal serupa dengan jenis data CNAME; tetapi, Anda dapat membuat alias untuk zone apex. Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Contoh untuk konsol Route 53

```
hostname.example.com
```

Contoh untuk API Route 53

```
<Value>hostname.example.com</Value>
```

Tipe catatan DS

Catatan delegasi penandatanganan (DS) merujuk kunci zona untuk zona subdomain yang didelegasikan. Anda dapat membuat data DS saat membuat rantai kepercayaan saat mengonfigurasi penandatanganan DNSSEC. Untuk informasi lebih lanjut tentang konfigurasi DNSSEC di Route 53, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

Tiga nilai pertama adalah angka desimal yang mewakili tanda kunci, algoritma, dan jenis digest. Nilai keempat adalah penyerapan kunci zona. Untuk informasi lebih lanjut tentang format catatan, lihat [RFC 4034](#).

Contoh untuk konsol Route 53

```
123 4 5 1234567890abcdef1234567890absdef
```

Contoh untuk API Route 53

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

Jenis catatan HTTPS

Catatan sumber daya HTTPS adalah bentuk catatan DNS Service Binding (SVCB) yang menyediakan informasi konfigurasi yang diperluas, memungkinkan klien untuk terhubung dengan mudah dan aman ke layanan dengan protokol HTTP. Informasi konfigurasi disediakan dalam parameter yang memungkinkan koneksi dalam satu kueri DNS, daripada memerlukan beberapa kueri DNS.

Format untuk catatan sumber daya HTTPS adalah:

`SvcPriority TargetName SvcParams(optional)`

Parameter berikut dijelaskan dalam [RFC 9460](#), bagian 9.1.

SvcPriority

Sebuah integer yang mewakili prioritas. 0 prioritas berarti modus alias, dan umumnya ditujukan untuk aliasing di puncak zona. Nilai ini adalah bilangan bulat 0-32767 untuk Route 53 dimana 1-32767 adalah catatan mode layanan. Turunkan prioritas, lebih tinggi preferensi.

TargetName

Nama domain dari target alias (untuk mode alias) atau titik akhir alternatif (untuk). ServiceMode
SvcParams (opsional)

Daftar yang dipisahkan spasi putih, dengan setiap parameter terdiri dari pasangan Key=Value atau kunci mandiri. Jika ada lebih dari satu nilai, mereka disajikan sebagai daftar yang dipisahkan koma. Berikut ini adalah yang didefinisikan SvcParams:

- `1:alpn`— Protokol Negosiasi IDs Protokol Lapisan Aplikasi. Defaultnya adalah HTTP/1.1, h2 HTTP/2 melalui TLS, dan h3 HTTP/3 (HTTP over QUIC protocol).
- `2:no-default-alpn`— Default tidak didukung dan Anda harus memberikan alpn parameter.
- `3:port`— titik akhir alternatif, atau port tempat layanan dapat dicapai.

- `4:ipv4hint`— petunjuk IPv4 alamat.
- `5:ech`— Klien Terenkripsi Halo.
- `6:ipv6hint`— petunjuk IPv6 alamat.
- `7:dohpath`— DNS melalui template HTTPS
- `8:http`— Layanan ini mengoperasikan target HTTP Oblivious

Contoh untuk konsol Amazon Route 53 untuk mode alias

```
0 example.com
```

Contoh untuk konsol Amazon Route 53 untuk mode layanan

```
16 example.com alpn="h2,h3" port=808
```

Contoh untuk Amazon Route 53 API untuk mode alias

```
<Value>0 example.com</Value>
```

Contoh untuk API Route 53 untuk mode layanan

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Untuk informasi selengkapnya, lihat [RFC 9460, Service Binding dan Spesifikasi Parameter melalui DNS \(SVCB dan HTTPS Resource Records\)](#).

Note

Route 53 tidak mendukung format presentasi kunci yang tidak diketahui sewenang-wenang `keyNNNNN`

Tipe catatan MX

Data MX menentukan nama server email Anda dan, jika Anda memiliki dua atau lebih server email, urutan prioritasnya. Setiap nilai untuk data MX berisi dua nilai, prioritas dan nama domain.

Prioritas

Bilangan bulat yang mewakili prioritas untuk server email. Jika Anda hanya menentukan satu server, prioritasnya dapat berupa bilangan bulat apa pun antara 0 dan 65535. Jika Anda menentukan beberapa server, nilai yang Anda tentukan untuk prioritas menunjukkan server email mana yang Anda inginkan untuk dirutekan ke email pertama, kedua, dan seterusnya. Server dengan nilai prioritas terendah didahulukan. Misalnya, jika Anda memiliki dua server email dan Anda menetapkan nilai 10 dan 20 untuk prioritas, email selalu masuk ke server dengan prioritas 10 kecuali jika tidak tersedia. Jika Anda menentukan nilai 10 dan 10, email dirutekan ke dua server kira-kira sama.

Nama domain

Nama domain server email. Tentukan nama (seperti mail.example.com) dari data A atau AAAA. Di bagian [RFC 2181, Klarifikasi ke Spesifikasi DNS, bagian 10.3](#) melarang menentukan nama catatan CNAME untuk nilai nama domain. (Ketika RFC menyebutkan "alias", itu berarti catatan CNAME, bukan catatan alias Route 53.)

Contoh untuk konsol Amazon Route 53

```
10 mail.example.com
```

Contoh untuk API Route 53

```
<Value>10 mail.example.com</Value>
```

Jenis catatan NAPTR

Name Authority Pointer (NAPTR) adalah jenis catatan yang digunakan oleh aplikasi Dynamic Delegation Discovery System (DDDS) untuk mengonversi satu nilai ke nilai lain atau mengganti satu nilai dengan nilai lainnya. Misalnya, salah satu penggunaan umum adalah mengubah nomor telepon menjadi SIP URIs.

Elemen `Value` untuk catatan NAPTR terdiri dari enam nilai yang dipisahkan oleh spasi:

Urutan

Saat Anda menentukan lebih dari satu catatan, urutan yang Anda inginkan agar aplikasi DDDS mengevaluasi catatan. Nilai yang valid: 0-65535.

Preferensi

Saat Anda menentukan dua atau lebih catatan yang memiliki Urutan yang sama, preferensi Anda untuk urutan yang dievaluasi dalam catatan tersebut. Misalnya, jika dua catatan memiliki Urutan 1, aplikasi DDDS pertama-tama mengevaluasi catatan yang memiliki Preferensi lebih rendah. Nilai yang valid: 0-65535.

Bendera

Pengaturan yang khusus untuk aplikasi DDDS. Nilai yang saat ini didefinisikan dalam [RFC 3404](#) adalah huruf besar dan huruf kecil "A", "P", "S", dan "U", dan string kosong, "". Sertakan Bendera dalam tanda petik.

Layanan

Pengaturan yang khusus untuk aplikasi DDDS. Sertakan Layanan dalam tanda petik.

Untuk informasi lebih lanjut, lihat yang berlaku RFCs:

- Aplikasi URI DDDS — <https://tools.ietf.org/html/rfc3404#section-4.4>
- Aplikasi S-NAPTR DDDS — [/rfc3958#section-6.5](#) <https://tools.ietf.org/html>
- Aplikasi U-NAPTR DDDS — [/rfc4848#section-4.5](#) <https://tools.ietf.org/html>

Regexp

Ekspresi reguler yang digunakan aplikasi DDDS untuk mengubah nilai input menjadi nilai output. Misalnya, sistem telepon IP mungkin menggunakan ekspresi reguler untuk mengonversi nomor telepon yang dimasukkan oleh pengguna menjadi URI SIP. Sertakan Regexp dalam tanda petik. Tentukan baik nilai untuk Regexp atau nilai untuk Pengganti, tetapi tidak keduanya.

Ekspresi reguler dapat menyertakan salah satu karakter ASCII yang dapat dicetak berikut ini:

- a-z
- 0-9
- - (tanda hubung)
- (spasi)
- ! # \$ % & ' () * + , - / : ; < = > ? @ [] ^ _ ` { | } ~ .
- " (tanda kutip). Untuk menyertakan kutipan literal dalam string, awali dengan \ karakter: \".
- \ (garis miring terbalik). Untuk menyertakan garis miring terbalik dalam string, awali dengan karakter \: \\\.

Tentukan semua nilai lainnya, seperti nama domain internasional, dalam format oktal.

Untuk sintaks untuk Regexp, lihat [RFC 3402, bagian 3.2, Sintaks Ekspresi Substitusi](#)

Pengganti

Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari nama domain berikutnya yang Anda inginkan agar aplikasi DDDS mengirimkan permintaan DNS. Aplikasi DDDS menggantikan nilai input dengan nilai yang Anda tentukan untuk Pengganti, jika ada. Tentukan baik nilai untuk Regexp atau nilai untuk Pengganti, tetapi tidak keduanya. Jika Anda menentukan nilai untuk Regexp, tentukan titik (.) untuk Penggantian.

Nama domain dapat menyertakan a-z, 0-9, dan - (tanda hubung).

Untuk informasi selengkapnya tentang aplikasi DDDS dan tentang catatan NAPTR, lihat berikut ini: RFCs

- [RFC 3401](#)
- [RFC 3402](#)
- [RFC 3403](#)
- [RFC 3404](#)

Contoh untuk konsol Amazon Route 53

```
100 50 "u" "E2U+sip" "!^(\\"+441632960083)$!sip:\\1@example.com!" .
100 51 "u" "E2U+h323" "!^(\\"+441632960083$!h323:operator@example.com!" .
100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .
```

Contoh untuk API Route 53

```
<ResourceRecord>
  <Value>100 50 "u" "E2U+sip" "!^(\\"+441632960083)$!sip:\\1@example.com!" .</Value>
  <Value>100 51 "u" "E2U+h323" "!^(\\"+441632960083$!h323:operator@example.com!" .</Value>
  <Value>100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .</Value>
</ResourceRecord>
```

Tipe catatan NS

Catatan NS mengidentifikasi server nama untuk zona yang di-hosting. Perhatikan hal berikut:

- Penggunaan paling umum untuk catatan NS adalah untuk mengontrol bagaimana lalu lintas internet dirutekan untuk suatu domain. Untuk menggunakan catatan di zona yang di-hosting untuk merutekan lalu lintas untuk domain, Anda memperbarui pengaturan pendaftaran domain untuk menggunakan empat server nama dalam catatan NS default. (Ini adalah catatan NS yang memiliki nama yang sama dengan zona yang di-hosting.)
- Anda dapat membuat zona yang di-hosting terpisah untuk subdomain (acme.example.com) dan menggunakan zona yang di-hosting tersebut untuk merutekan lalu lintas internet untuk subdomain dan subdomainnya (subdomain.acme.example.com). Anda menyiapkan konfigurasi ini, yang dikenal sebagai "mendelegasikan tanggung jawab untuk subdomain ke zona yang di-hosting" dengan membuat data NS lain di zona yang di-hosting untuk domain root (example.com). Untuk informasi selengkapnya, lihat [Merutekan lalu lintas untuk subdomain](#).
- Anda juga menggunakan data NS untuk mengonfigurasi server nama label putih. Untuk informasi selengkapnya, lihat [Mengonfigurasi server nama label putih](#).
- Penggunaan lain untuk catatan NS adalah untuk zona yang dihosting pribadi saat Anda membuat aturan delegasi untuk mendelegasikan otoritas subdomain ke resolver lokal Anda. Anda harus membuat catatan NS ini sebelum Anda membuat aturan delegasi. Untuk informasi selengkapnya, lihat [Bagaimana titik akhir Resolver meneruskan kueri DNS dari Anda ke jaringan Anda VPCs](#).

Untuk informasi lebih lanjut tentang catatan NS, lihat [Catatan NS dan SOA yang dibuat Amazon Route 53 untuk zona yang di-hosting publik](#).

Contoh untuk konsol Amazon Route 53

```
ns-1.example.com
```

Contoh untuk API Route 53

```
<Value>ns-1.example.com</Value>
```

Tipe catatan PTR

Catatan PTR memetakan alamat IP ke nama domain yang sesuai.

Contoh untuk konsol Amazon Route 53

```
hostname.example.com
```

Contoh untuk API Route 53

```
<Value>hostname.example.com</Value>
```

Jenis catatan SOA

Catatan awal otoritas (SOA) memberikan informasi tentang domain dan zona yang di-hosting Amazon Route 53 yang sesuai. Untuk informasi tentang bidang di catatan SOA, lihat [Catatan NS dan SOA yang dibuat Amazon Route 53 untuk zona yang di-hosting publik](#).

Contoh untuk konsol Route 53

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Contoh untuk API Route 53

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

Tipe catatan SPF

Catatan SPF sebelumnya digunakan untuk memverifikasi identitas pengirim pesan email. Namun, kami tidak lagi menyarankan Anda membuat catatan yang jenis catatannya adalah SPF. RFC 7208, Kerangka Kebijakan Pengirim (SPF) untuk Mengotorisasi Penggunaan Domain di Email, Versi 1, telah diperbarui untuk mengatakan, "... [I] keberadaan dan mekanisme yang didefinisikan dalam [RFC4408] telah menyebabkan beberapa masalah interoperabilitas. Dengan demikian, penggunaannya tidak lagi sesuai untuk SPF versi 1; implementasi tidak menggunakannya." Di RFC 7208, lihat bagian 14.1, [Jenis Catatan DNS SPF](#).

Sebagai ganti data SPF, sebaiknya Anda membuat data TXT yang berisi nilai yang berlaku. Untuk informasi selengkapnya tentang nilai yang valid, lihat artikel Wikipedia [Kerangka Kebijakan Pengirim](#).

Contoh untuk konsol Amazon Route 53

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Contoh untuk API Route 53

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Tipe catatan SRV

Elemen `Value` catatan SRV terdiri dari empat nilai yang dipisahkan oleh spasi. Tiga nilai pertama adalah angka desimal yang mewakili prioritas, bobot, dan port. Nilai keempat adalah nama domain. Catatan SRV digunakan untuk mengakses layanan, seperti layanan untuk email atau komunikasi. Untuk informasi tentang format catatan SRV, lihat dokumentasi untuk layanan yang ingin Anda sambungkan.

Contoh untuk konsol Amazon Route 53

```
10 5 80 hostname.example.com
```

Contoh untuk API Route 53

```
<Value>10 5 80 hostname.example.com</Value>
```

Jenis catatan SSHFP

Catatan sidik jari Secure Shell (SSHFP) mengidentifikasi kunci SSH yang terkait dengan nama domain. Catatan SSHFP harus diamankan dengan DNSSEC agar rantai kepercayaan dapat ditetapkan. Untuk informasi lebih lanjut tentang DNSSEC, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#)

Format untuk catatan sumber daya SSHFP adalah:

[Key Algorithm] [Hash Type] Fingerprint

Parameter berikut didefinisikan dalam [RFC 4255](#).

Algoritma Kunci

Jenis algoritma:

- 0— Dicadangkan dan tidak digunakan.
- 1: RSAAgoritma Rivest—Shamir—Adleman adalah salah satu kriptosistem kunci publik pertama dan masih digunakan untuk transmisi data yang aman.
- 2: DSAAgoritma Tanda Tangan Digital adalah Standar Pemrosesan Informasi Federal untuk tanda tangan digital. DSA didasarkan pada eksponensial modular dan model matematika logaritma diskrit.

- 3: ECDSA— Elliptic Curve Digital Signature Algorithm adalah varian dari DSA yang menggunakan kriptografi kurva elips.
- 4: Ed25519 Algoritma Ed25519 adalah skema tanda tangan eDDSA yang menggunakan SHA-512 (SHA-2) dan Curve25519.
- 6: Ed448- Ed448 adalah skema tanda tangan eDDSA yang menggunakan dan Curve448. SHAKE256

Jenis Hash

Algoritma yang digunakan untuk membuat hash kunci publik:

- 0—Dicadangkan dan tidak digunakan.
- 1: SHA-1
- 2: SHA-256

Sidik jari

Representasi heksadesimal dari hash.

Contoh untuk konsol Amazon Route 53

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Contoh untuk API Route 53

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

Untuk informasi selengkapnya, lihat [RFC 4255: Menggunakan DNS untuk Mempublikasikan Sidik Jari Kunci Secure Shell \(SSH\)](#) dengan Aman.

Jenis catatan SVCB

Anda menggunakan catatan SVCB untuk mengirimkan informasi konfigurasi untuk mengakses titik akhir layanan. SVCB adalah catatan DNS generik dan dapat digunakan untuk menegosiasikan parameter untuk berbagai protokol aplikasi.

Format untuk catatan sumber daya SVCB adalah:

SvcPriority TargetName SvcParams(optional)

Parameter berikut dijelaskan dalam [RFC 9460](#), bagian 2.3.

SvcPriority

Sebuah integer yang mewakili prioritas. 0 prioritas berarti modus alias, dan umumnya ditujukan untuk aliasing di puncak zona. Turunkan prioritas, lebih tinggi preferensi.

TargetName

Nama domain dari target alias (untuk mode alias) atau titik akhir alternatif (untuk). ServiceMode SvcParams (opsional)

Daftar yang dipisahkan spasi putih, dengan setiap parameter terdiri dari pasangan Key=Value atau kunci mandiri. Jika ada lebih dari satu nilai, mereka disajikan sebagai daftar yang dipisahkan koma. Nilai ini adalah bilangan bulat 0-32767 untuk Route 53 dimana 1-32767 adalah catatan mode layanan. Berikut ini adalah yang didefinisikan SvcParams:

- 1:alpn— Protokol Negosiasi IDs Protokol Lapisan Aplikasi. Defaultnya adalah HTTP/1.1, h2 HTTP/2 melalui TLS, dan h3 HTTP/3 (HTTP over QUIC protocol).
- 2:no-default-alpn— Default tidak didukung dan Anda harus memberikan alpn parameter.
- 3:port— port untuk titik akhir alternatif di mana layanan dapat dicapai.
- 4:ipv4hint— petunjuk IPv4 alamat.
- 5:ech— Klien Terenkripsi Halo.
- 6:ipv6hint— petunjuk IPv6 alamat.
- 7:dohpath— DNS melalui template HTTPS
- 8:http— Layanan ini mengoperasikan target HTTP Oblivious

Contoh untuk konsol Amazon Route 53 untuk mode alias

```
0 example.com
```

Contoh untuk konsol Amazon Route 53 untuk mode layanan

```
16 example.com alpn="h2,h3" port=808
```

Contoh untuk Amazon Route 53 API untuk mode alias

```
<Value>0 example.com</Value>
```

Contoh untuk API Route 53 untuk mode layanan

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Untuk informasi selengkapnya, lihat [RFC 9460, Service Binding dan Spesifikasi Parameter melalui DNS \(SVCB dan HTTPS Resource Records\)](#).

Note

Route 53 tidak mendukung format presentasi kunci yang tidak diketahui sewenang-wenang `keyNNNNN`

Jenis catatan TLSA

Anda menggunakan catatan TLSA untuk menggunakan Autentikasi Berbasis DNS dari Entitas Bernama (DANE). Catatan TLSA mengaitkan certificate/public kunci dengan titik akhir Transport Layer Security (TLS), dan klien dapat memvalidasi certificate/public kunci menggunakan catatan TLSA yang ditandatangani dengan DNSSEC.

Catatan TLSA hanya dapat dipercaya jika DNSSEC diaktifkan di domain Anda. Untuk informasi lebih lanjut tentang DNSSEC, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#)

Format untuk catatan sumber daya TLSA adalah:

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

Parameter berikut ditentukan dalam [RFC 6698, bagian 3](#).

Penggunaan sertifikat

Menentukan asosiasi yang disediakan yang akan digunakan untuk mencocokkan sertifikat yang disajikan dalam jabat tangan TLS:

- 0: CA Constraint — Sertifikat atau kunci publik harus ditemukan di jalur sertifikasi Public Key Infrastructure (PKIX) untuk sertifikat entitas akhir yang disediakan oleh server di TLS. Batasan batasan ini yang CAs dapat digunakan untuk menerbitkan sertifikat untuk layanan tertentu.
- 1: Kendala Sertifikat Layanan - Menentukan sertifikat entitas akhir (atau kunci publik) yang harus sesuai dengan sertifikat entitas akhir yang diberikan oleh server di TLS. Sertifikasi ini membatasi sertifikat entitas akhir mana yang dapat digunakan oleh layanan tertentu pada host.

- 2: Pernyataan Jangkar kepercayaan - Menentukan sertifikat (atau kunci publik) yang harus digunakan sebagai “jangkar kepercayaan” saat memvalidasi sertifikat entitas akhir yang diberikan oleh server di TLS. Memungkinkan administrator domain untuk menentukan jangkar kepercayaan.
- 3: Sertifikasi yang Diterbitkan Domain - Menentukan sertifikat (atau kunci publik) yang harus cocok dengan sertifikat entitas akhir yang diberikan oleh server di TLS. Sertifikasi ini memungkinkan administrator domain untuk mengeluarkan sertifikat untuk domain tanpa melibatkan CA pihak ketiga. Sertifikat ini tidak harus lulus validasi PKIX.

Pemilih

Menentukan bagian mana dari sertifikat yang disajikan oleh server dalam jabat tangan yang cocok dengan nilai asosiasi:

- 0: Seluruh sertifikat harus dicocokkan.
- 1: Kunci Publik Subjek, atau struktur biner yang dikodekan DER, harus dicocokkan.

Jenis pencocokan

Menentukan presentasi (sebagaimana ditentukan oleh bidang Selector) dari kecocokan sertifikat:

- 0: Pencocokan konten yang tepat.
- 1: SHA-256 hash.
- 2: SHA-512 hash.

Data asosiasi sertifikat

Data yang akan dicocokkan berdasarkan pengaturan bidang lainnya.

Contoh untuk konsol Amazon Route 53

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Contoh untuk API Route 53

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

Untuk informasi selengkapnya, lihat [RFC 6698, Protokol Transport Layer Security \(TLS\) Transport Layer Security \(DANE\) Berbasis DNS: TLSA](#).

Tipe catatan TXT

Catatan TXT berisi satu atau lebih string yang diapit dengan tanda petik ganda ("). Saat Anda menggunakan [kebijakan perutean](#) sederhana, sertakan semua nilai untuk domain (example.com) atau subdomain (www.example.com) dalam data TXT yang sama.

Topik

- [Memasukkan nilai catatan TXT](#)
- [Karakter khusus dalam nilai catatan TXT](#)
- [Huruf besar dan huruf kecil dalam nilai catatan TXT](#)
- [Contoh](#)

Memasukkan nilai catatan TXT

Satu string dapat berisi hingga 255 karakter, termasuk yang berikut:

- a-z
- A-Z
- 0-9
- Spasi
- - (tanda hubung)
- !"#\$%&'()*+,-/:;<=>?@[\\]^_`{|}~.

Jika Anda perlu memasukkan nilai yang lebih panjang dari 255 karakter, pisahkan nilai menjadi string 255 karakter atau kurang, dan sertakan setiap string dalam tanda kutip ganda ("). Di konsol, cantumkan semua string pada baris yang sama:

```
"String 1" "String 2" "String 3"
```

Untuk API, sertakan semua string dalam elemen `Value` yang sama:

```
<Value>"String 1" "String 2" "String 3"</Value>
```

Panjang maksimum nilai dalam data TXT adalah 4.000 karakter.

Untuk memasukkan lebih dari satu nilai TXT, masukkan satu nilai per baris.

Karakter khusus dalam nilai catatan TXT

Jika catatan TXT Anda berisi salah satu karakter berikut, Anda harus menentukan karakter dengan menggunakan kode escape dalam format: `\ three-digit octal code`

- Karakter 000 hingga 040 oktal (0 hingga 32 desimal, 0x00 hingga 0x20 heksadesimal)
- Karakter 177 hingga 377 oktal (127 hingga 255 desimal, 0x7F hingga 0xFF heksadesimal)

Misalnya, jika nilai data TXT Anda adalah "exämple.com", Anda menentukan "ex
\344mple.com".

Untuk pemetaan antara karakter ASCII dan kode oktal, lakukan pencarian internet untuk “kode oktal ASCII.” Satu referensi yang berguna adalah [Kode ASCII - Tabel ASCII yang diperluas](#).

Untuk menyertakan tanda kutip (") dalam sebuah string, letakkan karakter garis miring terbalik (\) sebelum tanda kutip: \".

Huruf besar dan huruf kecil dalam nilai catatan TXT

Kasus dipertahankan, sehingga "Ab" dan "aB" adalah nilai-nilai yang berbeda.

Contoh

Contoh untuk konsol Amazon Route 53

Letakkan setiap nilai pada baris terpisah:

```
"This string includes \"quotation marks\"."
"The last character in this string is an accented e specified in octal format: \351"
"v=spf1 ip4:192.168.0.1/16 -all"
```

Contoh untuk API Route 53

Letakkan setiap nilai dalam elemen Value terpisah:

```
<Value>"This string includes \"quotation marks\"."</Value>
<Value>"The last character in this string is an accented e specified in octal format:
 \351"</Value>
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Membuat catatan dengan menggunakan konsol Amazon Route 53

Prosedur berikut menjelaskan cara membuat catatan menggunakan konsol Amazon Route 53. Untuk informasi tentang cara membuat rekaman menggunakan API Route 53, lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.

Note

Untuk membuat catatan untuk konfigurasi perutean yang kompleks, Anda juga dapat menggunakan editor visual Aliran Lalu Lintas dan menyimpan konfigurasi sebagai kebijakan lalu lintas. Anda kemudian dapat mengaitkan kebijakan lalu lintas dengan satu atau lebih nama domain (seperti example.com) atau nama subdomain (seperti www.example.com), di zona yang di-hosting yang sama atau di beberapa zona yang di-hosting. Selain itu, Anda dapat memulihkan pembaruan jika konfigurasi baru tidak memiliki performa seperti yang Anda harapkan. Untuk informasi selengkapnya, lihat [Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS](#).

Untuk membuat catatan menggunakan konsol Route 53

1. Jika Anda tidak membuat catatan alias, lanjutkan ke langkah 2.

Juga pergi ke langkah 2 jika Anda membuat catatan alias yang merutekan lalu lintas DNS ke AWS sumber daya selain penyeimbang beban Elastic Load Balancing atau catatan Route 53 lainnya.

Jika Anda membuat catatan alias yang merutekan lalu lintas ke penyeimbang beban Elastic Load Balancing, dan jika Anda membuat zona yang dihosting dan penyeimbang beban menggunakan akun yang berbeda, lakukan [Mendapatkan nama DNS untuk penyeimbang beban Elastic Load Balancing](#) prosedur untuk mendapatkan nama DNS untuk penyeimbang beban.

2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Pada panel navigasi, pilih Zona yang di-hosting.
4. Jika Anda sudah memiliki zona yang di-hosting untuk domain Anda, lewati ke langkah 5. Jika belum, lakukan prosedur yang berlaku untuk membuat zona yang di-hosting:
 - Untuk merutekan lalu lintas internet ke sumber daya Anda, seperti bucket Amazon S3 atau EC2 instans Amazon, lihat. [Membuat zona yang di-hosting publik](#)

- Untuk merutekan lalu lintas di VPC Anda, lihat [Membuat zona yang di-hosting privat](#).
5. Pada halaman Zona yang di-hosting, pilih nama zona yang dihosting tempat Anda ingin membuat catatan.
 6. Pilih Buat catatan.
 7. Pilih dan tentukan kebijakan dan nilai perutean yang berlaku. Untuk informasi selengkapnya, lihat topik untuk jenis catatan yang ingin Anda buat:
 - [Nilai yang umum untuk semua kebijakan perutean](#)
 - [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)
 - [Nilai khusus untuk catatan sederhana](#)
 - [Nilai khusus untuk catatan alias sederhana](#)
 - [Nilai khusus untuk catatan failover](#)
 - [Nilai khusus untuk catatan alias failover](#)
 - [Nilai khusus untuk catatan geolokasi](#)
 - [Nilai khusus untuk catatan alias geolokasi](#)
 - [Nilai khusus untuk catatan geoproximity](#)
 - [Nilai khusus untuk catatan alias geoproximity](#)
 - [Nilai khusus untuk catatan latensi](#)
 - [Nilai khusus untuk catatan alias latensi](#)
 - [Nilai khusus untuk catatan berbasis IP](#)
 - [Nilai khusus untuk catatan alias berbasis IP](#)
 - [Nilai khusus untuk catatan jawaban multivalued](#)
 - [Nilai khusus untuk catatan tertimbang](#)
 - [Nilai khusus untuk catatan alias tertimbang](#)
 8. Pilih Create records (Buat catatan).

 Note

Catatan baru Anda membutuhkan waktu untuk menyebar ke server DNS Route 53. Saat ini, satu-satunya cara untuk memverifikasi bahwa perubahan telah disebarkan adalah dengan menggunakan tindakan [GetChangeAPI](#). Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

9. Jika Anda membuat beberapa catatan, ulangi langkah 7 hingga 8.

Mendapatkan nama DNS untuk penyeimbang beban Elastic Load Balancing

1. Masuk ke akun Konsol Manajemen AWS menggunakan AWS akun yang digunakan untuk membuat Classic, Application, atau Network Load Balancer yang ingin Anda buat catatan alias.
2. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
3. Di panel navigasi, pilih Load Balancers.
4. Dalam daftar penyeimbang beban, pilih penyeimbang beban yang ingin Anda buat data aliasnya.
5. Pada tab Deskripsi, dapatkan nilai Nama DNS.
6. Jika Anda ingin membuat catatan alias untuk penyeimbang beban Elastic Load Balancing lainnya, ulangi langkah 4 dan 5.
7. Keluar dari Konsol Manajemen AWS.
8. Masuk ke akun Konsol Manajemen AWS lagi menggunakan AWS akun yang Anda gunakan untuk membuat zona yang dihosting Route 53.
9. Kembali ke langkah 3 prosedur untuk [Membuat catatan dengan menggunakan konsol Amazon Route 53](#).

Izin set catatan sumber daya

Izin kumpulan catatan sumber daya menggunakan kondisi kebijakan Manajemen Identitas dan Akses (IAM) untuk memungkinkan Anda menetapkan izin terperinci untuk tindakan di konsol Route 53 atau untuk menggunakan API. [ChangeResourceRecordSets](#)

Kumpulan catatan sumber daya didefinisikan sebagai beberapa catatan sumber daya dengan nama dan jenis yang sama (dan kelas, tetapi untuk sebagian besar tujuan kelas selalu IN, atau internet), tetapi berisi data yang berbeda. Misalnya, jika Anda memilih perutean geolokasi, Anda dapat memiliki beberapa catatan A atau AAAA yang menunjuk ke titik akhir yang berbeda untuk domain yang sama. Semua catatan A atau AAAA ini bergabung untuk membentuk kumpulan catatan sumber daya. Untuk informasi lebih lanjut tentang terminologi DNS, lihat [RFC 7719](#).

Dengan ketentuan kebijakan

IAM, `route53:ChangeResourceRecordSetsNormalizedRecordNames`, dan

`route53:ChangeResourceRecordSetsRecordTypes` `route53:ChangeResourceRecordSetsActio`

Anda dapat memberikan hak administratif terperinci kepada AWS pengguna lain di akun lain AWS mana pun. Ini memungkinkan Anda memberikan izin kepada seseorang untuk:

- Satu set catatan sumber daya.
- Semua kumpulan catatan sumber daya dari jenis catatan DNS tertentu.
- Rekaman sumber daya menetapkan di mana nama berisi string tertentu.
- Lakukan salah satu, atau semua CREATE | UPSERT | DELETE tindakan saat menggunakan [ChangeResourceRecordSets](#) API, atau konsol Route 53.

Anda juga dapat membuat izin akses yang menggabungkan salah satu kondisi kebijakan Route 53. Misalnya, Anda dapat memberikan izin kepada seseorang untuk mengubah data catatan A untuk pemasaran-example.com, tetapi tidak mengizinkan pengguna tersebut untuk menghapus catatan apa pun.

Untuk informasi selengkapnya tentang izin kumpulan catatan sumber daya dan contoh cara menggunakannya, lihat [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#).

Untuk mempelajari cara mengautentikasi AWS pengguna, lihat [Mengautentikasi dengan identitas](#) dan mempelajari cara mengontrol akses ke sumber daya Route 53, lihat [Kontrol akses](#).

Nilai yang Anda tentukan saat membuat atau mengedit catatan Amazon Route 53

Saat Anda membuat rekaman menggunakan konsol Amazon Route 53, nilai yang Anda tentukan bergantung pada kebijakan perutean yang ingin Anda gunakan dan apakah Anda membuat catatan alias, yang merutekan lalu lintas ke AWS sumber daya.

Alias mencatat lalu lintas yang merutekan lalu lintas ke AWS sumber daya tertentu yang Anda tentukan sumber daya targetnya (misalnya, Elastic Load Balancing CloudFront , distribusi, bucket Amazon S3). Anda juga dapat secara opsional mengaitkan pemeriksaan kesehatan dan mengonfigurasi evaluasi kesehatan target. Topik berikut memberikan informasi terperinci tentang nilai yang diperlukan untuk setiap kebijakan perutean dan jenis rekaman, membantu Anda mengonfigurasi catatan Route 53 Anda secara efektif.

Topik

- [Nilai yang umum untuk semua kebijakan perutean](#)
- [Nilai yang umum untuk catatan alias untuk semua kebijakan perutean](#)

- [Nilai khusus untuk catatan sederhana](#)
- [Nilai khusus untuk catatan alias sederhana](#)
- [Nilai khusus untuk catatan failover](#)
- [Nilai khusus untuk catatan alias failover](#)
- [Nilai khusus untuk catatan geolokasi](#)
- [Nilai khusus untuk catatan alias geolokasi](#)
- [Nilai khusus untuk catatan geoproximity](#)
- [Nilai khusus untuk catatan alias geoproximity](#)
- [Nilai khusus untuk catatan latensi](#)
- [Nilai khusus untuk catatan alias latensi](#)
- [Nilai khusus untuk catatan berbasis IP](#)
- [Nilai khusus untuk catatan alias berbasis IP](#)
- [Nilai khusus untuk catatan jawaban multivalued](#)
- [Nilai khusus untuk catatan tertimbang](#)
- [Nilai khusus untuk catatan alias tertimbang](#)

Nilai yang umum untuk semua kebijakan perutean

Ini adalah nilai umum yang dapat Anda tentukan saat membuat atau mengedit rekaman Amazon Route 53. Nilai-nilai ini digunakan oleh semua kebijakan routing.

Topik

- [Nama catatan](#)
- [Menilai/Merutekan lalu lintas](#)
- [TTL \(detik\)](#)

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

 Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Catatan CNAME

Jika Anda membuat catatan yang memiliki nilai CNAME untuk Jenis catatan, nama catatan tidak dapat sama dengan nama zona yang di-hosting.

Karakter-karakter khusus

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

Karakter wildcard

Anda dapat menggunakan karakter tanda bintang (*) dalam nama. DNS memperlakukan karakter * sebagai wildcard atau sebagai karakter * (ASCII 42), tergantung tempat karakter muncul dalam nama. Untuk informasi selengkapnya, lihat [Menggunakan tanda bintang \(*\) dalam nama zona yang di-hosting dan catatan](#).

 Important

Anda tidak dapat menggunakan wildcard * untuk set catatan sumber daya yang memiliki tipe NS.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

A — IPv4 alamat

Alamat IP dalam IPv4 format, misalnya, 192.0.2.235.

AAAA — alamat IPv6

Alamat IP dalam IPv6 format, misalnya, 2001:0 db 8:85 a 3:0:0:8 a2e: 0370:7334.

CAA — Otorisasi Otoritas Sertifikat

Tiga nilai yang dipisahkan spasi yang mengontrol otoritas sertifikat mana yang diizinkan untuk menerbitkan sertifikat atau sertifikat wildcard untuk domain atau subdomain yang ditentukan oleh Nama catatan. Anda dapat menggunakan catatan CAA untuk menentukan hal berikut:

- Otoritas sertifikat mana (CAs) yang dapat mengeluarkan sertifikat SSL/TLS, jika ada
- Alamat email atau URL untuk dihubungi saat CA mengeluarkan sertifikat untuk domain atau subdomain

CNAME — Nama kanonis

Nama domain yang sepenuhnya memenuhi syarat (misalnya, `www.example.com`) yang Anda inginkan untuk dihasilkan oleh Route 53 sebagai tanggapan atas kueri DNS untuk catatan ini. Titik akhir adalah opsional; Route 53 mengasumsikan bahwa nama domain sepenuhnya memenuhi syarat. Ini berarti bahwa Route 53 memperlakukan `www.example.com` (tanpa titik akhir) dan `www.example.com.` (dengan titik akhir) sebagai identik.

MX — Pertukaran surat

Prioritas dan nama domain yang menentukan server email, misalnya, `10 mailserver.example.com`. Titik trailing diperlakukan sebagai opsional.

NAPTR - Nama Authority Pointer

Enam pengaturan dipisahkan ruang yang digunakan oleh Dynamic Delegation Discovery System (DDDS) aplikasi untuk mengonversi satu nilai lain atau untuk mengganti satu nilai dengan yang lain. Untuk informasi selengkapnya, lihat [Jenis catatan NAPTR](#).

PTR — Pointer

Nama domain yang Anda inginkan untuk dihasilkan Route 53.

NS — Server nama

Nama domain dari server nama, misalnya, `ns1.example.com`.

Note

Anda dapat menentukan catatan NS hanya dengan kebijakan perutean sederhana.

SPF — Kerangka Kebijakan Pengirim

Catatan SPF yang diapit tanda kutip, misalnya, "v=spf1 ip4:192.168.0.1/16-all". Catatan SPF tidak disarankan. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

SRV — Locator layanan

Catatan SRV. Catatan SRV digunakan untuk mengakses layanan, seperti layanan untuk email atau komunikasi. Untuk informasi tentang format catatan SRV, lihat dokumentasi untuk layanan yang ingin Anda sambungkan. Trailing dot diperlakukan sebagai opsional.

Format catatan SRV adalah:

[prioritas] [berat] [port] [nama host server]

Sebagai contoh:

1 10 5269 xmpp-server.example.com.

TXT — Teks

Catatan teks. Lampirkan teks dalam tanda kutip, sebagai contoh, ""Contoh entri teks".

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Nilai yang umum untuk catatan alias untuk semua kebijakan perutean

Ini adalah nilai alias umum yang dapat Anda tentukan saat membuat atau mengedit rekaman Amazon Route 53. Nilai-nilai ini digunakan oleh semua kebijakan routing.

Topik

- [Nama catatan](#)
- [Menilai/Merutekan lalu lintas](#)

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Catatan CNAME

Jika Anda membuat catatan yang memiliki nilai CNAME untuk Jenis, nama catatan tidak boleh sama dengan nama zona yang di-hosting.

Alias untuk CloudFront distribusi dan bucket Amazon S3

Nilai yang Anda tentukan sebagian bergantung pada AWS sumber daya yang Anda rutekan lalu lintas ke:

- CloudFront distribusi — Distribusi Anda harus menyertakan nama domain alternatif yang cocok dengan nama catatan. Misalnya, jika nama catatan adalah acme.example.com, CloudFront distribusi Anda harus menyertakan acme.example.com sebagai salah satu nama domain alternatif. Untuk informasi selengkapnya, lihat [Menggunakan nama domain alternatif \(CNAMEs\)](#) di Panduan CloudFront Pengembang Amazon.
- Bucket Amazon S3 – Nama catatan harus sesuai dengan nama bucket Amazon S3 Anda. Misalnya, jika nama bucket Anda acme.example.com, nama catatan ini juga harus acme.example.com.

Selain itu, Anda harus mengonfigurasi bucket untuk meng-host situs web. Untuk informasi selengkapnya, lihat [Mengonfigurasi bucket untuk hosting situs web](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Karakter-karakter khusus

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

Karakter wildcard

Anda dapat menggunakan karakter tanda bintang (*) dalam nama. DNS memperlakukan karakter * sebagai wildcard atau sebagai karakter * (ASCII 42), tergantung tempat karakter muncul dalam nama. Untuk informasi selengkapnya, lihat [Menggunakan tanda bintang \(*\) dalam nama zona yang di-hosting dan catatan](#).

Menilai/Merutekan lalu lintas

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Important

Jika Anda menggunakan AWS akun yang sama untuk membuat zona yang dihosting dan sumber daya yang Anda rutekan lalu lintas, dan jika sumber daya Anda tidak muncul di daftar Titik Akhir, periksa hal berikut:

- Konfirmasi bahwa Anda memilih nilai yang didukung untuk Jenis catatan. Nilai yang didukung khusus untuk sumber daya tempat Anda merutekan lalu lintas. Misalnya, untuk merutekan lalu lintas ke bucket S3, Anda harus memilih IPv4 alamat A — untuk jenis Rekam.
- Konfirmasikan bahwa akun memiliki izin IAM yang diperlukan untuk mencantumkan sumber daya yang berlaku. Misalnya, agar CloudFront distribusi muncul di daftar Titik Akhir, akun harus memiliki izin untuk melakukan tindakan berikut:
`cloudfront:ListDistributions`

Untuk contoh kebijakan IAM, lihat [izin diperlukan untuk menggunakan konsol Amazon Route 53](#).

Jika Anda menggunakan AWS akun yang berbeda untuk membuat zona yang dihosting dan sumber daya, daftar Endpoint tidak menampilkan sumber daya Anda. Lihat dokumentasi berikut untuk jenis sumber daya Anda untuk menentukan nilai yang akan diketik di Titik Akhir.

API Gateway khusus regional APIs dan dioptimalkan tepi APIs

Untuk API Gateway kustom regional APIs dan edge-optimize APIs, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona yang di-hosting Route 53 dan API Anda – Pilih Endpoint (Titik Akhir), lalu pilih API dari daftar. Jika Anda memiliki banyak APIs, Anda dapat memasukkan beberapa karakter pertama dari titik akhir API untuk memfilter daftar.

Note

Nama data ini harus cocok dengan nama domain khusus untuk API Anda, seperti `api.example.com`.

- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang di-hosting Route 53 dan API Anda— Masukkan titik akhir API untuk API, seperti `api.example.com`.

Jika Anda menggunakan satu AWS akun untuk membuat zona host saat ini dan akun lain untuk membuat API, API tidak akan muncul di daftar Titik Akhir di bawah API Gateway APIs.

Jika Anda menggunakan satu akun untuk membuat zona host saat ini dan satu atau beberapa akun berbeda untuk membuat semua akun Anda APIs, daftar Titik Akhir akan menampilkan Tidak ada target yang tersedia di bawah API Gateway APIs. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke API Amazon API Gateway dengan menggunakan nama domain Anda](#).

CloudFront distribusi

Untuk CloudFront distribusi, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona yang dihosting Route 53 dan CloudFront distribusi Anda — Pilih Titik Akhir dan pilih distribusi dari daftar. Jika Anda memiliki

banyak distribusi, Anda dapat memasukkan beberapa karakter pertama dari nama domain untuk distribusi Anda untuk memfilter daftar.

Jika distribusi Anda tidak muncul dalam daftar, perhatikan hal berikut:

- Nama catatan ini harus cocok dengan nama domain alternatif di distribusi Anda.
- Jika Anda baru saja menambahkan nama domain alternatif ke distribusi Anda, mungkin diperlukan waktu 15 menit agar perubahan Anda menyebar ke semua lokasi CloudFront tepi. Sampai perubahan menyebar, Route 53 tidak dapat mengetahui tentang nama domain alternatif yang baru.
- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang dihosting Route 53 dan distribusi Anda — Masukkan nama CloudFront domain untuk distribusi, seperti `d111111abcdef8.cloudfront.net`.

Jika Anda menggunakan satu AWS akun untuk membuat zona host saat ini dan akun lain untuk membuat distribusi, distribusi tidak akan muncul di daftar Endpoints.

Jika Anda menggunakan satu akun untuk membuat zona yang dihosting saat ini dan satu atau beberapa akun berbeda untuk membuat semua distribusi, daftar Titik Akhir menunjukkan Tidak ada target yang tersedia di bawah CloudFront distribusi.

Important

Jangan merutekan kueri ke CloudFront distribusi yang belum disebar ke semua lokasi tepi, atau pengguna Anda tidak akan dapat mengakses konten yang berlaku.

CloudFront Distribusi Anda harus menyertakan nama domain alternatif yang cocok dengan nama catatan. Misalnya, jika nama catatan adalah `acme.example.com`, CloudFront distribusi Anda harus menyertakan `acme.example.com` sebagai salah satu nama domain alternatif. Untuk informasi selengkapnya, lihat [Menggunakan nama domain alternatif \(CNAMEs\)](#) di Panduan CloudFront Pengembang Amazon.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk jenis Rekaman, dan satu dengan nilai AAAA — IPv6 alamat. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#).

Layanan Pelari Aplikasi

Untuk layanan App Runner, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona yang dihosting Route 53 dan layanan App Runner Anda — pilih Wilayah AWS, lalu pilih nama domain lingkungan tempat Anda ingin mengarahkan lalu lintas dari daftar.
- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang dihosting Route 53 dan Pelari Aplikasi Anda — Masukkan nama domain khusus. Untuk informasi selengkapnya, lihat [Mengelola nama domain khusus untuk App Runner](#).

Jika Anda menggunakan satu AWS akun untuk membuat zona yang dihosting saat ini dan akun lain untuk membuat Pelari Aplikasi, Pelari Aplikasi tidak akan muncul di daftar Titik Akhir.

Untuk informasi selengkapnya, lihat [Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke layanan App Runner](#).

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Jika nama domain untuk lingkungan Elastic Beanstalk Anda menyertakan Wilayah tempat Anda menerapkan lingkungan, Anda dapat membuat catatan alias yang merutekan lalu lintas ke lingkungan. Sebagai contoh, nama domain `my-environment.us-west-2.elasticbeanstalk.com` adalah nama domain regional.

Important

Untuk lingkungan yang dibuat sebelum awal 2016, nama domain tidak termasuk Wilayah. Untuk merutekan lalu lintas ke lingkungan ini, Anda harus membuat catatan CNAME, alih-alih catatan alias. Perhatikan bahwa Anda tidak dapat membuat catatan CNAME untuk nama domain root. Misalnya, jika nama domain Anda adalah `example.com`, Anda dapat membuat catatan yang mengarahkan lalu lintas untuk `acme.example.com` ke lingkungan Elastic Beanstalk Anda, tetapi Anda tidak dapat membuat catatan yang mengarahkan lalu lintas untuk `example.com` ke lingkungan Elastic Beanstalk Anda.

Untuk lingkungan Elastic Beanstalk yang memiliki subdomain regional, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona yang di-hosting Route 53 dan lingkungan Elastic Beanstalk Anda – Pilih Endpoint (Titik akhir), lalu pilih lingkungan dari daftar. Jika Anda memiliki banyak lingkungan, Anda dapat memasukkan beberapa karakter pertama dari atribut CNAME untuk lingkungan guna memfilter daftar.

- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang di-hosting Route 53 dan lingkungan Elastic Beanstalk Anda – Masukkan atribut CNAME untuk lingkungan Elastic Beanstalk.

Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke lingkungan AWS Elastic Beanstalk](#).

Penyeimbang beban ELB

Di bagian penyeimbang beban ELB, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona yang di-hosting Route 53 dan penyeimbang beban Anda – Pilih Endpoint (Titik akhir) dan pilih penyeimbang beban dari daftar. Jika Anda memiliki banyak penyeimbang beban, Anda dapat memasukkan beberapa karakter pertama dari nama DNS untuk memfilter daftar.
- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang di-hosting Route 53 dan penyeimbang beban Anda – Masukkan nilai yang Anda dapatkan dalam prosedur [Mendapatkan nama DNS untuk penyeimbang beban Elastic Load Balancing](#).

Jika Anda menggunakan satu AWS akun untuk membuat zona host saat ini dan akun lain untuk membuat penyeimbang beban, penyeimbang beban tidak akan muncul di daftar Titik Akhir.

Jika Anda menggunakan satu akun untuk membuat zona yang dihosting saat ini dan satu atau beberapa akun berbeda untuk membuat semua penyeimbang beban Anda, daftar Titik Akhir menunjukkan Tidak ada target yang tersedia di bawah Elastic Load Balancers.

Konsol menambahkan dualstack. untuk Aplikasi dan Classic Load Balancer dari akun yang berbeda. Ketika klien, seperti browser web, meminta alamat IP untuk nama domain Anda (example.com) atau nama subdomain (www.example.com), klien dapat meminta alamat (catatan A), IPv4 alamat (catatan AAAA), atau keduanya IPv4 dan IPv6 alamat (dalam permintaan terpisah). IPv6 Penunjukan dualstack. memungkinkan Route 53 untuk merespons dengan alamat IP yang sesuai untuk penyeimbang beban Anda berdasarkan format alamat IP yang diminta klien.

Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke penyeimbang beban ELB](#).

AWS Akselerator Akselerator Global

Untuk akselerator AWS Global Accelerator, masukkan nama DNS untuk akselerator. Anda dapat memasukkan nama DNS akselerator yang Anda buat menggunakan AWS akun saat ini atau menggunakan akun lain AWS .

Bucket Amazon S3

Untuk bucket Amazon S3 yang dikonfigurasi sebagai titik akhir situs web, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona yang di-hosting Route 53 dan bucket Amazon S3 Anda – Pilih Endpoint (Titik Akhir) dan pilih bucket dari daftar. Jika Anda memiliki banyak bucket, Anda dapat memasukkan beberapa karakter pertama dari nama DNS untuk memfilter daftar.

Nilai Titik Akhir berubah ke titik akhir situs web Amazon S3 untuk bucket Anda.

- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang dihosting Route 53 dan bucket Amazon S3 Anda — Masukkan nama Wilayah tempat Anda membuat bucket S3. Gunakan nilai yang muncul di kolom titik akhir Situs Web dalam tabel titik akhir [situs Amazon S3](#) di [Referensi Umum Amazon Web Services](#)

Jika Anda menggunakan AWS akun selain akun saat ini untuk membuat bucket Amazon S3, bucket tidak akan muncul di daftar Titik Akhir.

Anda dapat mengonfigurasi bucket untuk meng-host situs web. Untuk informasi selengkapnya, lihat [Mengonfigurasi bucket untuk hosting situs web](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Nama catatan harus cocok dengan nama bucket Amazon S3 Anda. Misalnya, jika nama bucket Amazon S3 Anda adalah `acme.example.com`, nama catatan ini juga harus `acme.example.com`.

Dalam grup catatan alias berbobot, alias latensi, alias failover, atau alias geolokasi, Anda hanya dapat membuat satu catatan yang merutekan kueri ke bucket Amazon S3 karena nama catatan harus cocok dengan nama bucket dan nama bucket harus unik secara global.

OpenSearch Layanan Amazon

Untuk OpenSearch Layanan, lakukan salah satu hal berikut:

- OpenSearch Domain kustom layanan: Nama catatan harus cocok dengan domain kustom. Misalnya, jika nama domain kustom Anda adalah `test.example.com`, nama catatan ini juga harus `test.example.com`.
- Jika Anda menggunakan akun yang sama untuk membuat zona host Route 53 dan domain OpenSearch Layanan Anda — pilih Wilayah AWS, lalu pilih nama domain.

- Jika Anda menggunakan akun yang berbeda untuk membuat zona yang dihosting Route 53 dan domain OpenSearch Layanan Anda — Masukkan nama domain khusus. Untuk informasi selengkapnya, lihat [Membuat titik akhir kustom](#).

Jika Anda menggunakan satu AWS akun untuk membuat zona host saat ini dan akun lain untuk membuat domain OpenSearch Layanan, domain tidak akan muncul dalam daftar Titik Akhir.

Jika Anda menggunakan satu akun untuk membuat zona yang dihosting saat ini dan satu atau beberapa akun berbeda untuk membuat semua domain OpenSearch Layanan Anda, daftar Titik Akhir menunjukkan Tidak ada target yang tersedia di bawah OpenSearch Layanan.

Untuk informasi selengkapnya, lihat [Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir domain OpenSearch Layanan Amazon](#).

Titik akhir antarmuka Amazon VPC

Untuk titik akhir antarmuka Amazon VPC, lakukan salah satu hal berikut:

- Jika Anda menggunakan akun yang sama untuk membuat zona host Route 53 dan titik akhir antarmuka Anda – Pilih Endpoint (Titik Akhir), lalu pilih titik akhir antarmuka dari daftar. Jika Anda memiliki banyak titik akhir antarmuka, Anda dapat memasukkan beberapa karakter pertama dari nama host DNS untuk memfilter daftar.
- Jika Anda menggunakan akun yang berbeda untuk membuat zona host Route 53 dan titik akhir antarmuka Anda — Masukkan nama host DNS untuk titik akhir antarmuka, seperti `vpce-123456789abcdef01-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com`. `example-us-east`

Jika Anda menggunakan satu AWS akun untuk membuat zona host saat ini dan akun lain untuk membuat titik akhir antarmuka, titik akhir antarmuka tidak akan muncul di daftar Titik Akhir di bawah titik akhir VPC.

Jika Anda menggunakan satu akun untuk membuat zona yang di-hosting saat ini dan satu atau beberapa akun berbeda untuk membuat semua titik akhir antarmuka Anda, daftar Titik Akhir menunjukkan Tidak ada target yang tersedia di VPC endpoint.

Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke titik akhir antarmuka Amazon Virtual Private Cloud dengan menggunakan nama domain Anda](#).

Catatan di Zona yang Di-hosting ini

Untuk rekaman di zona yang di-hosting ini, pilih Endpoint (Titik Akhir) dan pilih catatan yang berlaku. Jika Anda memiliki banyak catatan, Anda dapat memasukkan beberapa karakter pertama dari nama tersebut untuk memfilter daftar.

Jika zona yang di-hosting hanya berisi catatan NS dan SOA default, daftar Titik Akhir menunjukkan Tidak ada target yang tersedia.

Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang dihosting (dikenal sebagai zone apex), Anda tidak dapat memilih catatan dengan nilai Record type (Jenis catatan) adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Nilai khusus untuk catatan sederhana

Saat Anda membuat catatan sederhana, Anda menentukan nilai berikut.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Menilai/Merutekan lalu lintas](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)

Kebijakan perutean

Pilih Simple routing (Perutean sederhana).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6

- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- NS - Server nama

Nama domain dari server nama, misalnya, ns1.example.com.

 Note

Anda dapat menentukan catatan NS hanya dengan kebijakan perutean sederhana.

- PTR — Pointer
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan
- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai untuk Jenis catatan berdasarkan bagaimana Anda ingin Route 53 untuk menanggapi permintaan DNS.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta

Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Nilai khusus untuk catatan alias sederhana

Saat Anda membuat catatan alias, Anda menentukan nilai berikut. Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Note

Jika Anda menggunakan Route 53 di AWS GovCloud (US) Region, fitur ini memiliki beberapa batasan. Untuk informasi selengkapnya, lihat halaman [Amazon Route 53](#) di Panduan Pengguna AWS GovCloud (US) .

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Nilai/rutekan lalu lintas ke](#)
- [Jenis catatan](#)
- [Mengevaluasi Kondisi Target](#)

Kebijakan perutean

Pilih Simple routing (Perutean sederhana).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Nilai/rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya yang dapat Anda targetkan, lihat [nilai umum untuk catatan alias untuk value/route lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas ke:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan Pelari Aplikasi

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Bucket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buat alias. Semua jenis didukung kecuali NS dan SOA.

Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Mengevaluasi Kondisi Target

Ketika nilai Kebijakan perutean adalah Sederhana, Anda dapat memilih Tidak atau default Ya karena Mengevaluasi kondisi target tidak berpengaruh untuk perutean Sederhana. Jika Anda hanya memiliki satu catatan yang memiliki nama dan tipe tertentu, Route 53 merespons kueri DNS dengan menggunakan nilai dalam catatan tersebut terlepas dari apakah sumber dayanya sehat.

Untuk kebijakan perutean lainnya, Evaluasi kesehatan target menentukan apakah Route 53 memeriksa kesehatan sumber daya yang dirujuk oleh catatan alias:

- Layanan di mana Evaluasi kesehatan target memberikan manfaat operasional: Untuk penyeimbang beban (ELB) dan AWS Elastic Beanstalk lingkungan dengan penyeimbang beban, pengaturan Evaluasi kesehatan target ke Ya memungkinkan Route 53 untuk merutekan lalu lintas dari sumber daya yang tidak sehat.
- Layanan yang sangat tersedia: Untuk layanan seperti bucket Amazon S3, titik akhir antarmuka VPC, Amazon API Gateway, Amazon Service AWS Global Accelerator, dan Amazon VPC Lattice OpenSearch, Evaluate target health tidak memberikan manfaat operasional karena layanan ini dirancang untuk ketersediaan tinggi. Untuk skenario failover dengan layanan ini, gunakan [pemeriksaan kesehatan Route 53](#) sebagai gantinya.

Untuk informasi terperinci tentang cara kerja Evaluasi kesehatan target dengan berbagai AWS layanan, lihat [EvaluateTargetHealth](#) dokumentasi di referensi API.

Nilai khusus untuk catatan failover

Saat Anda membuat catatan failover, Anda menentukan nilai berikut.

Note

Untuk informasi tentang cara membuat catatan failover di zona yang di-hosting pribadi, lihat [Mengonfigurasi failover di zona yang di-hosting secara privat](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Tipe catatan failover](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Failover.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk kedua catatan dalam grup catatan failover.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang sama untuk catatan failover primer dan sekunder.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik

- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan
- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Tipe catatan failover

Pilih nilai yang berlaku untuk catatan ini. Agar failover berfungsi dengan benar, Anda harus membuat satu catatan failover primer dan satu sekunder.

Anda tidak dapat membuat rekaman non-failover yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan failover.

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Rute 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.

- Anda memilih Ya untuk Mengevaluasi Kesehatan Target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama Domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

 Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan primer dan sekunder.

Nilai khusus untuk catatan alias failover

Ketika Anda membuat catatan alias failover, Anda menentukan nilai-nilai berikut.

Untuk informasi, lihat topik berikut:

- Untuk informasi tentang membuat rekaman failover di zona yang di-hosting pribadi, lihat [Mengonfigurasi failover di zona yang di-hosting secara privat](#).
- Untuk informasi tentang catatan alias, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Tipe catatan](#)
- [Nilai/Rutekan lalu lintas ke](#)
- [Tipe catatan failover](#)
- [Pemeriksaan kondisi](#)
- [Mengevaluasi Kondisi Target](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Failover.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk kedua catatan dalam grup catatan failover.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Tipe catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas. Pilih nilai yang sama untuk catatan failover primer dan sekunder:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan Pelari Aplikasi

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Buket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buatkan alias. Semua jenis didukung kecuali NS dan SOA.

 Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Nilai/Rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya yang dapat Anda targetkan, lihat [nilai umum untuk catatan alias untuk value/route lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

 Note

Saat Anda membuat catatan failover primer dan sekunder, Anda dapat secara opsional membuat satu failover dan satu catatan alias failover yang memiliki nilai yang sama untuk Nama dan Jenis catatan. Jika Anda mencampur failover dan failover alias catatan, salah satunya bisa menjadi catatan utama.

Tipe catatan failover

Pilih nilai yang berlaku untuk catatan ini. Agar failover berfungsi dengan benar, Anda harus membuat satu catatan failover primer dan satu sekunder.

Anda tidak dapat membuat rekaman non-failover yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan failover.

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi Kesehatan Target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama Domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Mengevaluasi Kondisi Target

Pilih Ya jika Anda ingin Route 53 untuk menentukan apakah untuk menanggapi permintaan DNS menggunakan catatan ini dengan memeriksa kondisi sumber daya yang ditentukan oleh Titik akhir.

Perhatikan hal-hal berikut:

API Gateway khusus regional APIs dan dioptimalkan tepi APIs

Tidak ada persyaratan khusus untuk menyetel Evaluasi kondisi target ke Ya ketika titik akhir adalah API regional kustom API Gateway atau API yang dioptimalkan edge.

CloudFront distribusi

Anda tidak dapat menetapkan Evaluasi kesehatan target ke Ya ketika titik akhir adalah CloudFront distribusi.

Lingkungan Elastic Beanstalk yang memiliki subdomain regionalisasi

Jika Anda menentukan lingkungan Elastic Beanstalk di Endpoint dan lingkungan berisi penyeimbang beban ELB, Elastic Load Balancing akan merutekan kueri hanya ke instans Amazon sehat yang terdaftar dengan penyeimbang beban. EC2 (Lingkungan secara otomatis berisi penyeimbang beban ELB jika menyertakan lebih dari satu EC2 instans Amazon.) Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instans Amazon yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain yang tersedia yang sehat, jika ada.

Jika lingkungan berisi satu EC2 instance Amazon, tidak ada persyaratan khusus.

penyeimbang beban ELB

Perilaku pemeriksaan kondisi tergantung pada jenis penyeimbang beban:

- Penyeimbang beban klasik - Jika Anda menentukan ELB Classic Load Balancer di Endpoint, Elastic Load Balancing hanya akan mengarahkan kueri ke instans EC2 Amazon sehat yang terdaftar dengan penyeimbang beban. Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instance yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain.
- Aplikasi dan Penyeimbang Beban Jaringan – Jika Anda menentukan Aplikasi ELB atau Penyeimbang Beban Jaringan dan Anda menyetel Evaluasi kondisi target ke Ya, Route 53 merutekan kueri ke penyeimbang beban berdasarkan kondisi grup target yang terkait dengan penyeimbang beban:

- Agar Aplikasi atau Network Load Balancer dianggap sehat, kelompok sasaran yang berisi target harus mengandung setidaknya satu target yang sehat. Jika setiap kelompok target hanya berisi target yang tidak sehat, penyeimbang beban dianggap tidak sehat, dan Route 53 merutekan permintaan ke sumber daya lainnya.
- Grup target yang tidak memiliki target terdaftar dianggap tidak sehat.

 Note

Bila Anda membuat penyeimbang beban, Anda mengonfigurasi pengaturan untuk pemeriksaan kondisi Elastic Load Balancing; bukan pemeriksaan kondisi Route 53, tetapi melakukan fungsi serupa. Jangan membuat pemeriksaan kesehatan Route 53 untuk EC2 kasus yang Anda daftarkan dengan penyeimbang beban ELB.

Bucket S3

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah bucket S3.

Titik akhir antarmuka Amazon VPC

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah antarmuka Amazon VPC.

Catatan lain di zona yang di-hosting

Jika AWS sumber daya yang Anda tentukan di Endpoint adalah rekaman atau grup catatan (misalnya, grup catatan tertimbang) tetapi bukan catatan alias lain, sebaiknya Anda mengaitkan pemeriksaan kesehatan dengan semua catatan di titik akhir. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#).

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan primer dan sekunder.

Nilai khusus untuk catatan geolokasi

Saat Anda membuat catatan geolokasi, Anda menentukan nilai berikut.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Lokasi](#)
- [Negara bagian AS](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Geolocation (Geolokasi).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Masukkan nama yang sama untuk semua catatan dalam grup catatan geolokasi.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang sama untuk semua catatan dalam grup catatan geolokasi.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan

- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Lokasi

Saat Anda mengonfigurasi Route 53 untuk merespons kueri DNS berdasarkan lokasi asal kueri, pilih benua atau negara yang Anda inginkan agar Route 53 merespons dengan pengaturan dalam catatan ini. Jika Anda ingin Route 53 merespons kueri DNS untuk masing-masing negara bagian di Amerika Serikat, pilih United States (Amerika Serikat) dari daftar Location (Lokasi), lalu pilih negara bagian di bagian grup Sublocation (Sublokasi).

Untuk zona host pribadi, pilih benua, negara, atau sub-divisi Wilayah AWS yang paling dekat dengan tempat sumber daya Anda berada. Misalnya, jika sumber daya Anda ada di us-east-1, Anda dapat menentukan Amerika Utara, Amerika Serikat, atau Virginia.

Important

Kami merekomendasikan agar Anda membuat satu data geolokasi yang memiliki nilai Default untuk Lokasi. Ini mencakup lokasi geografis yang catatannya belum Anda buat dan alamat IP yang lokasinya tidak dapat diidentifikasi oleh Route 53.

Anda tidak dapat membuat catatan nongeolokasi yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan geolokasi.

Untuk informasi selengkapnya, lihat [Perutean geolokasi](#).

Berikut adalah negara-negara yang Amazon Route 53 kaitkan dengan setiap benua. Kode negara berasal dari ISO 3166. Untuk informasi lebih lanjut, lihat artikel Wikipedia [ISO 3166-1 alpha-2](#):

Afrika (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antartika (AN)

AQ, GS, TF

Asia (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

Eropa (Uni Eropa)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

Note

Beberapa penyedia menganggap TR berada di Asia dan alamat IP akan mencerminkan hal itu.

Amerika Utara (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Oseania (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

Amerika Selatan (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 tidak mendukung pembuatan catatan geolokasi untuk negara-negara berikut: Pulau Bouvet (BV), Pulau Natal (CX), Sahara Barat (EH), dan Pulau dan Kepulauan Heard (HM).
McDonald Tidak ada data yang tersedia mengenai alamat IP untuk negara-negara ini.

Negara bagian AS

Jika Anda mengonfigurasi Route 53 untuk merespons permintaan DNS berdasarkan keadaan Amerika Serikat tempat asal kueri, pilih negara dari daftar Negara bagian AS. Wilayah Amerika Serikat (misalnya, Puerto Riko) terdaftar sebagai negara di daftar Lokasi.

Important

Beberapa alamat IP dikaitkan dengan Amerika Serikat, tetapi tidak dengan negara bagian individual. Jika Anda membuat catatan untuk semua negara bagian di Amerika Serikat, kami menyarankan Anda juga membuat catatan untuk Amerika Serikat untuk merutekan kueri untuk alamat IP yang tidak terkait ini. Jika Anda tidak membuat catatan untuk Amerika Serikat, Route 53 merespons kueri DNS dari alamat IP Amerika Serikat yang tidak terkait dengan pengaturan dari catatan geolokasi default (jika Anda membuatnya) atau dengan respons "tidak ada jawaban".

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.

- Anda memilih Ya untuk Mengevaluasi Kesehatan Target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama Domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

 Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Untuk catatan geolokasi, jika titik akhir tidak sehat, Route 53 mencari catatan untuk Wilayah geografis terkait yang lebih besar. Misalnya, Anda memiliki catatan untuk negara bagian di Amerika Serikat, Amerika Serikat, Amerika Utara, dan untuk semua lokasi (Lokasi adalah Default). Jika titik akhir untuk catatan negara bagian tidak sehat, Route 53 memeriksa catatan untuk Amerika Serikat, Amerika Utara, dan untuk semua lokasi, dalam urutan itu, hingga menemukan catatan yang memiliki titik akhir yang sehat. Jika semua rekaman yang berlaku tidak sehat, termasuk catatan untuk semua lokasi, Route 53 merespons kueri DNS menggunakan nilai catatan untuk wilayah geografis terkecil.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan geolokasi.

Nilai khusus untuk catatan alias geolokasi

Saat Anda membuat catatan alias geolokasi, Anda menentukan nilai berikut.

Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Tipe catatan](#)
- [Nilai/Rutekan lalu lintas ke](#)
- [Lokasi](#)
- [Negara bagian AS](#)
- [Pemeriksaan kondisi](#)
- [Mengevaluasi Kondisi Target](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Geolocation (Geolokasi).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan geolokasi.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Tipe catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas. Pilih nilai yang sama untuk semua catatan dalam grup catatan geolokasi:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan Pelari Aplikasi

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Buket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buatkan alias. Semua jenis didukung kecuali NS dan SOA.

 Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan

dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Nilai/Rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya apa yang dapat Anda targetkan, lihat [Menilai/Merutekan lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Lokasi

Saat Anda mengonfigurasi Route 53 untuk merespons kueri DNS berdasarkan lokasi asal kueri, pilih benua atau negara yang Anda inginkan agar Route 53 merespons dengan pengaturan dalam catatan ini. Jika Anda ingin Route 53 merespons kueri DNS untuk masing-masing negara bagian di Amerika Serikat, pilih United States (Amerika Serikat) dari daftar Location (Lokasi), lalu pilih negara bagian dari daftar U.S. states (negara bagian AS).

Untuk zona host pribadi, pilih benua, negara, atau sub-divisi Wilayah AWS yang paling dekat dengan tempat sumber daya Anda berada. Misalnya, jika sumber daya Anda ada di us-east-1, Anda dapat menentukan Amerika Utara, Amerika Serikat, atau Virginia.

Important

Kami merekomendasikan agar Anda membuat satu data geolokasi yang memiliki nilai Default untuk Lokasi. Ini mencakup lokasi geografis yang catatannya belum Anda buat dan alamat IP yang lokasinya tidak dapat diidentifikasi oleh Route 53.

Anda tidak dapat membuat catatan nongeolokasi yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan geolokasi.

Untuk informasi selengkapnya, lihat [Perutean geolokasi](#).

Berikut adalah negara-negara yang Amazon Route 53 kaitkan dengan setiap benua. Kode negara berasal dari ISO 3166. Untuk informasi lebih lanjut, lihat artikel Wikipedia [ISO 3166-1 alpha-2](#):

Afrika (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antartika (AN)

AQ, GS, TF

Asia (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

Eropa (Uni Eropa)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

Note

Beberapa penyedia menganggap TR berada di Asia dan alamat IP akan mencerminkan hal itu.

Amerika Utara (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Oseania (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

Amerika Selatan (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

 Note

Route 53 tidak mendukung pembuatan catatan geolokasi untuk negara-negara berikut: Pulau Bouvet (BV), Pulau Natal (CX), Sahara Barat (EH), dan Pulau dan Kepulauan Heard (HM). McDonald Tidak ada data yang tersedia mengenai alamat IP untuk negara-negara ini.

Negara bagian AS

Jika Anda mengonfigurasi Route 53 untuk merespons permintaan DNS berdasarkan keadaan Amerika Serikat tempat asal kueri, pilih negara dari daftar Negara bagian AS. Wilayah Amerika Serikat (misalnya, Puerto Riko) terdaftar sebagai negara di daftar Lokasi.

 Important

Beberapa alamat IP dikaitkan dengan Amerika Serikat, tetapi tidak dengan negara bagian individual. Jika Anda membuat catatan untuk semua negara bagian di Amerika Serikat, kami menyarankan Anda juga membuat catatan untuk Amerika Serikat untuk merutekan kueri untuk alamat IP yang tidak terkait ini. Jika Anda tidak membuat catatan untuk Amerika Serikat, Route 53 merespons kueri DNS dari alamat IP Amerika Serikat yang tidak terkait dengan pengaturan dari catatan geolokasi default (jika Anda membuatnya) atau dengan respons "tidak ada jawaban".

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Untuk catatan geolokasi, jika titik akhir tidak sehat, Route 53 mencari catatan untuk Wilayah geografis terkait yang lebih besar. Misalnya, Anda memiliki catatan untuk negara bagian di Amerika Serikat, Amerika Serikat, Amerika Utara, dan untuk semua lokasi (Lokasi adalah Default). Jika titik akhir untuk catatan negara bagian tidak sehat, Route 53 memeriksa catatan untuk Amerika Serikat, Amerika Utara, dan untuk semua lokasi, dalam urutan itu, hingga menemukan catatan yang memiliki titik akhir yang sehat. Jika semua rekaman yang berlaku tidak sehat, termasuk catatan untuk semua lokasi, Route 53 merespons kueri DNS menggunakan nilai catatan untuk wilayah geografis terkecil.

Mengevaluasi Kondisi Target

Pilih Ya jika Anda ingin Route 53 untuk menentukan apakah untuk menanggapi permintaan DNS menggunakan catatan ini dengan memeriksa kondisi sumber daya yang ditentukan oleh Titik akhir.

Perhatikan hal-hal berikut:

API Gateway khusus regional APIs dan dioptimalkan tepi APIs

Tidak ada persyaratan khusus untuk menyetel Evaluasi kesehatan target ke Ya ketika titik akhir adalah API Regional kustom API Gateway API atau API yang dioptimalkan tepi.

CloudFront distribusi

Anda tidak dapat menetapkan Evaluasi kesehatan target ke Ya ketika titik akhir adalah CloudFront distribusi.

Lingkungan Elastic Beanstalk yang memiliki subdomain regionalisasi

Jika Anda menentukan lingkungan Elastic Beanstalk di Endpoint dan lingkungan berisi penyeimbang beban ELB, Elastic Load Balancing akan merutekan kueri hanya ke instans Amazon sehat yang terdaftar dengan penyeimbang beban. EC2 (Lingkungan secara otomatis berisi penyeimbang beban ELB jika menyertakan lebih dari satu EC2 instans Amazon.) Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instans Amazon yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain yang tersedia yang sehat, jika ada.

Jika lingkungan berisi satu EC2 instance Amazon, tidak ada persyaratan khusus.

penyeimbang beban ELB

Perilaku pemeriksaan kondisi tergantung pada jenis penyeimbang beban:

- **Classic Load Balancers** — Jika Anda menentukan ELB Classic Load Balancer di Endpoint, Elastic Load Balancing akan merutekan kueri hanya ke instans EC2 Amazon sehat yang terdaftar dengan penyeimbang beban. Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instance yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 merutekan kueri ke sumber daya lain.
- **Aplikasi dan Penyeimbang Beban Jaringan** – Jika Anda menentukan Aplikasi ELB atau Penyeimbang Beban Jaringan dan Anda menyetel Evaluasi kondisi target ke Ya, Route 53 merutekan kueri ke penyeimbang beban berdasarkan kondisi grup target yang terkait dengan penyeimbang beban:

- Agar Aplikasi atau Penyeimbang Beban Jaringan dianggap sehat, setiap kelompok target yang berisi target harus berisi setidaknya satu target yang sehat. Jika setiap kelompok target hanya berisi target yang tidak sehat, penyeimbang beban dianggap tidak sehat, dan Route 53 merutekan permintaan ke sumber daya lainnya.
- Grup target yang tidak memiliki target terdaftar dianggap tidak sehat.

 Note

Bila Anda membuat penyeimbang beban, Anda mengonfigurasi pengaturan untuk pemeriksaan kondisi Elastic Load Balancing; bukan pemeriksaan kondisi Route 53, tetapi melakukan fungsi serupa. Jangan membuat pemeriksaan kesehatan Route 53 untuk EC2 kasus yang Anda daftarkan dengan penyeimbang beban ELB.

Bucket S3

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah bucket S3.

Titik akhir antarmuka Amazon VPC

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah antarmuka Amazon VPC.

Catatan lain di zona yang di-hosting

Jika AWS sumber daya yang Anda tentukan di Endpoint adalah rekaman atau grup catatan (misalnya, grup catatan tertimbang) tetapi bukan catatan alias lain, sebaiknya Anda mengaitkan pemeriksaan kesehatan dengan semua catatan di titik akhir. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#).

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan geolokasi.

Nilai khusus untuk catatan geoproximity

Saat Anda membuat catatan geoproximity, Anda menentukan nilai berikut.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Lokasi titik akhir](#)
- [Bias](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Geoproximity.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Masukkan nama yang sama untuk semua catatan dalam grup catatan geoproximity.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang sama untuk semua catatan dalam kelompok catatan geoproximity.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan

- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Lokasi titik akhir

Anda dapat menentukan lokasi titik akhir sumber daya dengan menggunakan salah satu dari berikut ini:

Koordinat kustom

Tentukan garis bujur dan garis lintang untuk area geografi.

Wilayah AWS

Pilih Wilayah yang tersedia dari daftar Lokasi.

Untuk informasi selengkapnya tentang Wilayah, lihat [Infrastruktur AWS Global](#).

AWS Grup Zona Lokal

Pilih Grup Zona Lokal yang tersedia dari daftar Lokasi.

Untuk informasi selengkapnya tentang Local Zones, lihat [Available Local Zones](#) di Panduan Pengguna AWS Local Zones. Grup Zona lokal biasanya adalah Zona Lokal tanpa karakter akhir. Misalnya, jika Zona Lokal adalah us-east-1-bue-1a Grup Zona Lokal us-east-1-bue-1.

Anda juga dapat mengidentifikasi Grup Local Zones untuk Zona Lokal tertentu dengan menggunakan perintah [describe-availability-zones](#) CLI:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Perintah ini mengembalikan: "GroupName": "us-west-2-den-1", menentukan bahwa Zona Lokal us-west-2-den-1a milik Grup us-west-2-den-1 Zona Lokal.

Anda tidak dapat membuat rekaman non-geoproximity yang memiliki nilai yang sama untuk nama Rekam dan jenis Rekam sebagai catatan geoproximity.

Anda juga tidak dapat membuat dua kumpulan rekaman sumber daya geoproximity yang menentukan lokasi yang sama untuk nama rekaman dan jenis rekaman yang sama.

Bias

Bias memperluas atau menyusutkan wilayah geografis dari mana Rute 53 merutekan lalu lintas ke sumber daya. Bias positif memperluas area, dan bias negatif menyusutkannya. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menggunakan bias untuk merutekan lalu lintas](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Rute 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi Kesehatan Target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias geoproximity, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi

untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama Domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

 Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Untuk catatan geoproximity, jika titik akhir tidak sehat, Route 53 mencari titik akhir terdekat yang masih sehat.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam kelompok catatan geoproximity.

Nilai khusus untuk catatan alias geoproximity

Saat Anda membuat catatan alias geoproximity, Anda menentukan nilai berikut.

Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Tipe catatan](#)
- [Nilai/Rutekan lalu lintas ke](#)
- [Lokasi titik akhir](#)
- [Bias](#)
- [Pemeriksaan kondisi](#)
- [Mengevaluasi Kondisi Target](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Geoproximity.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan geoproximity.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Tipe catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas. Pilih nilai yang sama untuk semua catatan dalam grup catatan geoproximity:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan App Runner

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Buket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buatkan alias. Semua jenis didukung kecuali NS dan SOA.

 Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan

dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Nilai/Rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya apa yang dapat Anda targetkan, lihat [Menilai/Merutekan lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Lokasi titik akhir

Anda dapat menentukan lokasi titik akhir sumber daya dengan menggunakan salah satu dari berikut ini:

Koordinat kustom

Tentukan garis bujur dan garis lintang untuk area geografi.

Wilayah AWS

Pilih Wilayah yang tersedia dari daftar Lokasi.

Untuk informasi selengkapnya tentang Wilayah, lihat [Infrastruktur AWS Global](#).

AWS Grup Zona Lokal

Pilih Wilayah Zona Lokal yang tersedia dari daftar Lokasi.

Untuk informasi selengkapnya tentang Local Zones, lihat [Available Local Zones](#) di Panduan Pengguna AWS Local Zones. Grup Zona lokal biasanya adalah Zona Lokal tanpa karakter akhir. Misalnya, jika Zona Lokal adalah us-east-1-bue-1a Grup Zona Lokal us-east-1-bue-1.

Anda juga dapat mengidentifikasi Grup Local Zones untuk Zona Lokal tertentu dengan menggunakan perintah [describe-availability-zones](#) CLI:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Perintah ini mengembalikan: "GroupName": "us-west-2-den-1", menentukan bahwa Zona Lokal us-west-2-den-1a milik Grup us-west-2-den-1 Zona Lokal.

Anda tidak dapat membuat rekaman non-geoproximity yang memiliki nilai yang sama untuk nama Rekam dan jenis Rekam sebagai catatan geoproximity.

Anda juga tidak dapat membuat dua kumpulan rekaman sumber daya geoproximity yang menentukan lokasi yang sama untuk nama rekaman dan jenis rekaman yang sama.

Untuk informasi lebih lanjut, [available-local-zones lihat.html](#)

Bias

Bias memperluas atau menyusutkan wilayah geografis dari mana Rute 53 merutekan lalu lintas ke sumber daya. Bias positif memperluas area, dan bias negatif menyusutkannya. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menggunakan bias untuk merutekan lalu lintas](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Rute 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk

catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.

- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias geoproximity, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Untuk catatan geoproximity, jika titik akhir tidak sehat, Route 53 mencari titik akhir terdekat yang masih sehat.

Mengevaluasi Kondisi Target

Pilih Ya jika Anda ingin Route 53 untuk menentukan apakah untuk menanggapi permintaan DNS menggunakan catatan ini dengan memeriksa kondisi sumber daya yang ditentukan oleh Titik akhir.

Perhatikan hal-hal berikut:

API Gateway khusus regional APIs dan dioptimalkan di tepi APIs

Tidak ada persyaratan khusus untuk menyetel Evaluasi kesehatan target ke Ya ketika titik akhir adalah API Regional kustom API Gateway API atau API yang dioptimalkan tepi.

CloudFront distribusi

Anda tidak dapat menetapkan Evaluasi kesehatan target ke Ya ketika titik akhir adalah CloudFront distribusi.

Lingkungan Elastic Beanstalk yang memiliki subdomain regionalisasi

Jika Anda menentukan lingkungan Elastic Beanstalk di Endpoint dan lingkungan berisi penyeimbang beban ELB, Elastic Load Balancing akan merutekan kueri hanya ke instans Amazon sehat yang terdaftar dengan penyeimbang beban. EC2 (Lingkungan secara otomatis berisi penyeimbang beban ELB jika menyertakan lebih dari satu EC2 instans Amazon.) Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instans Amazon yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain yang tersedia yang sehat, jika ada.

Jika lingkungan berisi satu EC2 instance Amazon, tidak ada persyaratan khusus.

penyeimbang beban ELB

Perilaku pemeriksaan kondisi tergantung pada jenis penyeimbang beban:

- **Classic Load Balancers** — Jika Anda menentukan ELB Classic Load Balancer di Endpoint, Elastic Load Balancing akan merutekan kueri hanya ke instans EC2 Amazon sehat yang terdaftar dengan penyeimbang beban. Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instance yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 merutekan kueri ke sumber daya lain.
- **Aplikasi dan Penyeimbang Beban Jaringan** – Jika Anda menentukan Aplikasi ELB atau Penyeimbang Beban Jaringan dan Anda menyetel Evaluasi kondisi target ke Ya, Route 53 merutekan kueri ke penyeimbang beban berdasarkan kondisi grup target yang terkait dengan penyeimbang beban:
 - Agar Aplikasi atau Penyeimbang Beban Jaringan dianggap sehat, setiap kelompok target yang berisi target harus berisi setidaknya satu target yang sehat. Jika setiap kelompok target hanya berisi target yang tidak sehat, penyeimbang beban dianggap tidak sehat, dan Route 53 merutekan permintaan ke sumber daya lainnya.
 - Grup target yang tidak memiliki target terdaftar dianggap tidak sehat.

Note

Bila Anda membuat penyeimbang beban, Anda mengonfigurasi pengaturan untuk pemeriksaan kondisi Elastic Load Balancing; bukan pemeriksaan kondisi Route 53, tetapi

melakukan fungsi serupa. Jangan membuat pemeriksaan kesehatan Route 53 untuk EC2 kasus yang Anda daftarkan dengan penyeimbang beban ELB.

Bucket S3

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah bucket S3.

Titik akhir antarmuka Amazon VPC

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah antarmuka Amazon VPC.

Catatan lain di zona yang di-hosting

Jika AWS sumber daya yang Anda tentukan di Endpoint adalah rekaman atau grup catatan (misalnya, grup catatan tertimbang) tetapi bukan catatan alias lain, sebaiknya Anda mengaitkan pemeriksaan kesehatan dengan semua catatan di titik akhir. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#).

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam kelompok catatan geoproximity.

Nilai khusus untuk catatan latensi

Saat Anda membuat data latensi, Anda menentukan nilai berikut.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Wilayah](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Latency (Latensi).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan latensi.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai untuk Jenis berdasarkan bagaimana Anda ingin Route 53 untuk menanggapi permintaan DNS.

Pilih nilai yang sama untuk semua rekaman dalam grup rekaman latensi.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim

- SRV - Pencari lokasi layanan
- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Wilayah

EC2 Wilayah Amazon tempat sumber daya yang Anda tentukan dalam catatan ini berada. Route 53 merekomendasikan EC2 Wilayah Amazon berdasarkan nilai lain yang telah Anda tentukan. Ini juga berlaku untuk zona yang dihosting pribadi. Kami menyarankan Anda untuk tidak mengubah nilai ini.

Perhatikan hal berikut:

- Anda hanya dapat membuat satu catatan latensi untuk setiap EC2 Wilayah Amazon.
- Anda tidak diharuskan membuat catatan latensi untuk semua EC2 Wilayah Amazon. Route 53 memilih Wilayah dengan latensi terbaik dari antara Wilayah tempat Anda membuat catatan latensi.
- Anda tidak dapat membuat rekaman nonlatensi yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan latensi.
- Jika Anda membuat rekaman yang ditandai dengan Region cn-north-1, Route 53 selalu menanggapi kueri dari dalam Tiongkok menggunakan catatan ini, terlepas dari latensinya.

Untuk informasi lebih lanjut tentang penggunaan catatan latensi, lihat [Perutean berbasis latensi](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Rute 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

 Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan latensi.

Nilai khusus untuk catatan alias latensi

Saat Anda membuat catatan alias latensi, Anda menentukan nilai berikut.

Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Tipe catatan](#)
- [Nilai/Rutekan lalu lintas ke](#)
- [Region](#)
- [Pemeriksaan kondisi](#)
- [Mengevaluasi Kondisi Target](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Latency (Latensi).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan latensi.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#)

Tipe catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas ke:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan App Runner

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Buket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buatkan alias. Semua jenis didukung kecuali NS dan SOA.

Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Pilih nilai yang sama untuk semua rekaman dalam grup rekaman latensi.

Nilai/Rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya yang dapat Anda targetkan, lihat [nilai umum untuk catatan alias untuk value/route lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Region

EC2 Wilayah Amazon tempat sumber daya yang Anda tentukan dalam catatan ini berada. Route 53 merekomendasikan EC2 Wilayah Amazon berdasarkan nilai lain yang telah Anda tentukan. Ini juga berlaku untuk zona yang dihosting pribadi. Kami menyarankan Anda untuk tidak mengubah nilai ini.

Perhatikan hal-hal berikut:

- Anda hanya dapat membuat satu catatan latensi untuk setiap EC2 Wilayah Amazon.
- Anda tidak diharuskan membuat catatan latensi untuk semua EC2 Wilayah Amazon. Route 53 memilih Wilayah dengan latensi terbaik dari berbagai Wilayah yang Anda buat catatan latensinya.
- Anda tidak dapat membuat rekaman nonlatensi yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan latensi.
- Jika Anda membuat catatan yang ditandai dengan Wilayah cn-north-1, Route 53 akan selalu merespons kueri yang berasal dari Tiongkok menggunakan catatan ini, terlepas dari latensinya.

Untuk informasi lebih lanjut tentang penggunaan catatan latensi, lihat [Perutean berbasis latensi](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi

tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Mengevaluasi Kondisi Target

Pilih Ya jika Anda ingin Route 53 untuk menentukan apakah untuk menanggapi permintaan DNS menggunakan catatan ini dengan memeriksa kondisi sumber daya yang ditentukan oleh Titik akhir.

Perhatikan hal-hal berikut:

API Gateway khusus regional APIs dan dioptimalkan di tepi APIs

Tidak ada persyaratan khusus untuk menyetel Evaluasi kondisi target ke Ya ketika titik akhir adalah API regional kustom API Gateway atau API yang dioptimalkan edge.

CloudFront distribusi

Anda tidak dapat mengatur Evaluate Target Health ke Yes ketika titik akhir adalah CloudFront distribusi.

Lingkungan Elastic Beanstalk yang memiliki subdomain regionalisasi

Jika Anda menentukan lingkungan Elastic Beanstalk di Endpoint dan lingkungan berisi penyeimbang beban ELB, Elastic Load Balancing akan merutekan kueri hanya ke instans Amazon sehat yang terdaftar dengan penyeimbang beban. EC2 (Lingkungan secara otomatis berisi penyeimbang beban ELB jika menyertakan lebih dari satu EC2 instans Amazon.) Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instans Amazon yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain yang tersedia yang sehat, jika ada.

Jika lingkungan berisi satu EC2 instance Amazon, tidak ada persyaratan khusus.

penyeimbang beban ELB

Perilaku pemeriksaan kondisi tergantung pada jenis penyeimbang beban:

- Classic Load Balancers — Jika Anda menentukan ELB Classic Load Balancer di Endpoint, Elastic Load Balancing akan merutekan kueri hanya ke instans EC2 Amazon sehat yang terdaftar dengan penyeimbang beban. Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instance yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 merutekan kueri ke sumber daya lain.
- Aplikasi dan Penyeimbang Beban Jaringan – Jika Anda menentukan Aplikasi ELB atau Penyeimbang Beban Jaringan dan Anda menyetel Evaluasi kondisi target ke Ya, Route 53 merutekan kueri ke penyeimbang beban berdasarkan kondisi grup target yang terkait dengan penyeimbang beban:
 - Agar Aplikasi atau Penyeimbang Beban Jaringan dianggap sehat, setiap kelompok target yang berisi target harus berisi setidaknya satu target yang sehat. Jika setiap kelompok target hanya berisi target yang tidak sehat, penyeimbang beban dianggap tidak sehat, dan Route 53 merutekan permintaan ke sumber daya lainnya.

- Grup target yang tidak memiliki target terdaftar dianggap tidak sehat.

 Note

Bila Anda membuat penyeimbang beban, Anda mengonfigurasi pengaturan untuk pemeriksaan kondisi Elastic Load Balancing; bukan pemeriksaan kondisi Route 53, tetapi melakukan fungsi serupa. Jangan membuat pemeriksaan kesehatan Route 53 untuk EC2 kasus yang Anda daftarkan dengan penyeimbang beban ELB.

Bucket S3

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah bucket S3.

Titik akhir antarmuka Amazon VPC

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah antarmuka Amazon VPC.

Catatan lain di zona yang di-hosting

Jika AWS sumber daya yang Anda tentukan di Endpoint adalah rekaman atau grup catatan (misalnya, grup catatan tertimbang) tetapi bukan catatan alias lain, sebaiknya Anda mengaitkan pemeriksaan kesehatan dengan semua catatan di titik akhir. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#).

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan latensi.

Nilai khusus untuk catatan berbasis IP

Saat Anda membuat catatan berbasis IP, Anda menentukan nilai berikut.

Note

Meskipun membuat catatan berbasis IP di zona host pribadi diperbolehkan, itu tidak didukung.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Lokasi](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih berbasis IP.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan berbasis IP.

Catatan CNAME

Jika Anda membuat catatan yang memiliki nilai CNAME untuk Jenis catatan, nama catatan tidak dapat sama dengan nama zona yang di-hosting.

Karakter-karakter khusus

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

Karakter wildcard

Anda dapat menggunakan karakter tanda bintang (*) dalam nama. DNS memperlakukan karakter * sebagai wildcard atau sebagai karakter * (ASCII 42), tergantung tempat karakter muncul dalam nama. Untuk informasi selengkapnya, lihat [Menggunakan tanda bintang \(*\) dalam nama zona yang di-hosting dan catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai untuk Jenis berdasarkan bagaimana Anda ingin Route 53 untuk menanggapi permintaan DNS.

Pilih nilai yang sama untuk semua catatan dalam grup catatan berbasis IP.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan
- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai Menilai/Merutekan lalu lintas umum untuk lalu lintas Nilai/Rute ke](#).

Lokasi

Nama lokasi CIDR di mana sumber daya yang Anda tentukan dalam catatan ini ditentukan oleh nilai blok CIDR dalam lokasi CIDR.

Untuk informasi selengkapnya tentang penggunaan catatan berbasis IP, lihat [Perutean berbasis IP](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan,

Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias berbasis IP, alias latensi, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam kelompok catatan berbasis IP.

Nilai khusus untuk catatan alias berbasis IP

Saat Anda membuat catatan alias berbasis IP, Anda menentukan nilai berikut.

Note

Meskipun membuat catatan alias berbasis IP di zona host pribadi diizinkan, itu tidak didukung.

Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [Nilai/Rutekan lalu lintas ke](#)
- [Lokasi](#)
- [Pemeriksaan kondisi](#)
- [Mengevaluasi Kondisi Target](#)
- [ID catatan](#)

Kebijakan perutean

Pilih berbasis IP.

Note

Meskipun membuat catatan alias berbasis IP di zona host pribadi diizinkan, itu tidak didukung.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

 Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan berbasis IP.

Catatan CNAME

Jika Anda membuat catatan yang memiliki nilai CNAME untuk Jenis catatan, nama catatan tidak dapat sama dengan nama zona yang di-hosting.

Alias untuk CloudFront distribusi dan bucket Amazon S3

Nilai yang Anda tentukan sebagian bergantung pada AWS sumber daya yang Anda rutekan lalu lintas ke:

- CloudFront distribusi — Distribusi Anda harus menyertakan nama domain alternatif yang cocok dengan nama catatan. Misalnya, jika nama catatan adalah `acme.example.com`, CloudFront distribusi Anda harus menyertakan `acme.example.com` sebagai salah satu nama domain alternatif. Untuk informasi selengkapnya, lihat [Menggunakan nama domain alternatif \(CNAMEs\)](#) di Panduan CloudFront Pengembang Amazon.
- Bucket Amazon S3 – Nama catatan harus sesuai dengan nama bucket Amazon S3 Anda. Misalnya, jika nama bucket Anda `acme.example.com`, nama catatan ini juga harus `acme.example.com`.

Selain itu, Anda harus mengonfigurasi bucket untuk meng-host situs web. Untuk informasi selengkapnya, lihat [Mengonfigurasi bucket untuk hosting situs web](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Karakter-karakter khusus

Untuk informasi tentang cara menentukan karakter selain a-z, 0-9, dan - (tanda hubung) serta cara menentukan nama domain internasional, lihat [Format nama domain DNS](#).

Karakter wildcard

Anda dapat menggunakan karakter tanda bintang (*) dalam nama. DNS memperlakukan karakter * sebagai wildcard atau sebagai karakter * (ASCII 42), tergantung tempat karakter muncul dalam nama. Untuk informasi selengkapnya, lihat [Menggunakan tanda bintang \(*\) dalam nama zona yang di-hosting dan catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas. Pilih nilai yang sama untuk semua catatan dalam grup catatan berbasis IP:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan App Runner

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Buket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buatkan alias. Semua jenis didukung kecuali NS dan SOA.

 Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Nilai/Rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya yang dapat Anda targetkan, lihat [nilai umum untuk catatan alias untuk value/route lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Lokasi

Saat Anda mengonfigurasi Route 53 untuk menanggapi kueri DNS berdasarkan lokasi asal kueri, pilih lokasi CIDR yang Anda inginkan untuk merespons Route 53 dengan pengaturan dalam catatan ini.

 Important

Sebaiknya buat satu catatan berbasis IP yang memiliki nilai Default untuk Lokasi. Ini mencakup lokasi yang belum Anda buat catatan dan alamat IP yang Route 53 tidak dapat mengidentifikasi lokasinya.

Anda tidak dapat membuat non-IP-based rekaman yang memiliki nilai yang sama untuk nama Rekam dan jenis Rekam sebagai catatan berbasis IP.

Untuk informasi selengkapnya, lihat [Perutean berbasis IP](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias perutean berbasis IP, alias latensi, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Untuk catatan alias berbasis IP, jika titik akhir tidak sehat, Route 53 mencari catatan di dalam lokasi yang lebih besar dan terkait. Misalnya, Anda memiliki catatan untuk negara bagian di Amerika Serikat, Amerika Serikat, Amerika Utara, dan untuk semua lokasi (Lokasi adalah Default). Jika titik akhir untuk catatan negara bagian tidak sehat, Route 53 memeriksa catatan untuk Amerika Serikat, Amerika Utara, dan untuk semua lokasi, dalam urutan itu, hingga menemukan catatan yang memiliki titik akhir yang sehat. Jika semua rekaman yang berlaku tidak sehat, termasuk catatan untuk semua lokasi, Route 53 merespons kueri DNS menggunakan nilai catatan untuk wilayah geografis terkecil.

Mengevaluasi Kondisi Target

Pilih Ya jika Anda ingin Route 53 untuk menentukan apakah untuk menanggapi permintaan DNS menggunakan catatan ini dengan memeriksa kondisi sumber daya yang ditentukan oleh Titik akhir.

Perhatikan hal-hal berikut:

API Gateway khusus regional APIs dan dioptimalkan di tepi APIs

Tidak ada persyaratan khusus untuk menyetel Evaluasi kondisi target ke Ya ketika titik akhir adalah API regional kustom API Gateway atau API yang dioptimalkan edge.

CloudFront distribusi

Anda tidak dapat menetapkan Evaluasi kesehatan target ke Ya ketika titik akhir adalah CloudFront distribusi.

Lingkungan Elastic Beanstalk yang memiliki subdomain regionalisasi

Jika Anda menentukan lingkungan Elastic Beanstalk di Endpoint dan lingkungan berisi penyeimbang beban ELB, Elastic Load Balancing akan merutekan kueri hanya ke instans Amazon sehat yang terdaftar dengan penyeimbang beban. EC2 (Lingkungan secara otomatis berisi penyeimbang beban ELB jika menyertakan lebih dari satu EC2 instans Amazon.) Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instans Amazon yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain yang tersedia yang sehat, jika ada.

Jika lingkungan berisi satu EC2 instance Amazon, tidak ada persyaratan khusus.

penyeimbang beban ELB

Perilaku pemeriksaan kondisi tergantung pada jenis penyeimbang beban:

- Classic Load Balancers — Jika Anda menentukan ELB Classic Load Balancer di Endpoint, Elastic Load Balancing akan merutekan kueri hanya ke instans EC2 Amazon sehat yang terdaftar dengan penyeimbang beban. Jika Anda menetapkan Evaluasi kesehatan target ke Ya

dan tidak ada EC2 instance yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 merutekan kueri ke sumber daya lain.

- Aplikasi dan Penyeimbang Beban Jaringan – Jika Anda menentukan Aplikasi ELB atau Penyeimbang Beban Jaringan dan Anda menyetel Evaluasi kondisi target ke Ya, Route 53 merutekan kueri ke penyeimbang beban berdasarkan kondisi grup target yang terkait dengan penyeimbang beban:
 - Agar Aplikasi atau Penyeimbang Beban Jaringan dianggap sehat, setiap kelompok target yang berisi target harus berisi setidaknya satu target yang sehat. Jika setiap kelompok target hanya berisi target yang tidak sehat, penyeimbang beban dianggap tidak sehat, dan Route 53 merutekan permintaan ke sumber daya lainnya.
 - Grup target yang tidak memiliki target terdaftar dianggap tidak sehat.

Note

Bila Anda membuat penyeimbang beban, Anda mengonfigurasi pengaturan untuk pemeriksaan kondisi Elastic Load Balancing; bukan pemeriksaan kondisi Route 53, tetapi melakukan fungsi serupa. Jangan membuat pemeriksaan kesehatan Route 53 untuk EC2 kasus yang Anda daftarkan dengan penyeimbang beban ELB.

Bucket S3

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah bucket S3.

Titik akhir antarmuka Amazon VPC

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah antarmuka Amazon VPC.

Catatan lain di zona yang di-hosting

Jika AWS sumber daya yang Anda tentukan di Endpoint adalah rekaman atau grup catatan (misalnya, grup catatan tertimbang) tetapi bukan catatan alias lain, sebaiknya Anda mengaitkan pemeriksaan kesehatan dengan semua catatan di titik akhir. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#)

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam kelompok catatan berbasis IP.

Nilai khusus untuk catatan jawaban multivalue

Saat Anda membuat catatan jawaban multinilai, Anda menentukan nilai berikut.

Note

Membuat catatan alias jawaban multinilai tidak didukung.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Multivalue answer (Jawaban multinilai).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam kelompok catatan multivalue.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai apapun kecuali NS atau CNAME.

Pilih nilai yang sama untuk semua catatan dalam grup catatan jawaban multinilai.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Note

Jika Anda membuat dua atau lebih catatan jawaban multivalue yang memiliki nama dan jenis yang sama, Anda menggunakan konsol, dan Anda menentukan nilai yang berbeda untuk TTL, Route 53 mengubah nilai TTL untuk semua catatan ke nilai terakhir yang Anda tentukan.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Jika Anda memasukkan lebih dari satu nilai, masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan
- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Rute 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Evaluasi kondisi target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, atau catatan alias berbobot. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan

pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

 Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan jawaban multinilai.

Nilai khusus untuk catatan tertimbang

Saat Anda membuat catatan tertimbang, Anda menentukan nilai berikut.

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Jenis catatan](#)
- [TTL \(detik\)](#)
- [Menilai/Merutekan lalu lintas](#)
- [Berat Badan](#)
- [Pemeriksaan kondisi](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Tertimbang.

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama catatan.

Masukkan nama yang sama untuk semua catatan dalam grup catatan tertimbang.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#).

Jenis catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang sama untuk semua catatan dalam kelompok grup tertimbang.

TTL (detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini memiliki efek mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Namun, jika Anda menentukan nilai yang lebih lama untuk TTL, diperlukan waktu lebih lama agar perubahan pada catatan (misalnya, alamat IP baru) diterapkan karena resolver rekursif menggunakan nilai dalam cache mereka untuk waktu yang lebih lama sebelum mereka meminta Route 53 untuk informasi terakhir. Jika Anda mengubah setelan untuk domain atau subdomain yang sudah digunakan, sebaiknya tentukan dulu nilai yang lebih pendek, seperti 300 detik, dan tingkatkan nilainya setelah mengonfirmasi bahwa pengaturan baru sudah benar.

Jika Anda mengaitkan catatan ini dengan pemeriksaan kondisi, sebaiknya tentukan TTL 60 detik atau kurang sehingga klien merespons dengan cepat perubahan status kondisi.

Anda harus menentukan nilai yang sama untuk TTL untuk semua catatan dalam grup catatan tertimbang ini.

Note

Jika Anda membuat dua atau lebih catatan tertimbang yang memiliki nama dan tipe yang sama, dan Anda menentukan nilai yang berbeda untuk TTL, Route 53 akan mengubah nilai TTL untuk semua catatan ke nilai terakhir yang Anda tentukan.

Jika grup catatan tertimbang menyertakan satu atau beberapa catatan alias tertimbang yang merutekan lalu lintas ke penyeimbang beban ELB, kami menyarankan agar Anda menentukan TTL 60 detik untuk semua catatan tertimbang nonalias yang memiliki nama dan tipe yang sama. Nilai selain 60 detik (TTL untuk penyeimbang beban) akan mengubah efek nilai yang Anda tentukan untuk Bobot.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan nilai yang sesuai untuk nilai Jenis catatan. Untuk semua jenis kecuali CNAME, Anda dapat memasukkan lebih dari satu nilai. Masukkan setiap nilai pada baris terpisah.

Anda dapat merutekan lalu lintas ke, atau menentukan nilai berikut:

- A — IPv4 alamat
- AAAA — alamat IPv6
- CAA - Otorisasi Otoritas Sertifikat
- CNAME — Nama kanonik
- MX - Pertukaran surat
- NAPTR - Penunjuk Otoritas Nama
- PTR — Penunjuk
- SPF - Kerangka Kebijakan Pengirim
- SRV - Pencari lokasi layanan
- TXT - Teks

Untuk informasi selengkapnya tentang nilai di atas, lihat [nilai umum untuk lalu lintas Nilai/Rute ke](#).

Berat Badan

Nilai yang menentukan proporsi kueri DNS yang ditanggapi oleh Route 53 menggunakan catatan saat ini. Route 53 menghitung jumlah bobot untuk catatan yang memiliki kombinasi yang sama dari nama dan jenis DNS. Route 53 kemudian merespons kueri berdasarkan rasio bobot sumber daya terhadap total.

Anda tidak dapat membuat catatan tidak tertimbang yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan tertimbang.

Masukkan bilangan bulat antara 0 dan 255. Untuk menonaktifkan perutean ke sumber daya, atur Bobot ke 0. Jika Anda menetapkan Bobot ke 0 untuk semua catatan dalam grup, lalu lintas dirutekan ke semua sumber daya dengan probabilitas yang sama. Hal ini memastikan bahwa Anda tidak secara tidak sengaja menonaktifkan perutean untuk grup catatan tertimbang.

Efek dari pengaturan Bobot ke 0 berbeda ketika Anda mengasosiasikan pemeriksaan kondisi dengan catatan tertimbang. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan tertimbang.

Nilai khusus untuk catatan alias tertimbang

Ketika Anda membuat catatan alias tertimbang, Anda menentukan nilai-nilai berikut. Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Topik

- [Kebijakan perutean](#)
- [Nama catatan](#)
- [Tipe catatan](#)
- [Nilai/Rutekan lalu lintas ke](#)
- [Bobot](#)
- [Pemeriksaan kondisi](#)
- [Mengevaluasi Kondisi Target](#)
- [ID catatan](#)

Kebijakan perutean

Pilih Weighted (Tertimbang).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda tuju lalu lintasnya. Nilai default adalah nama zona yang di-hosting.

Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Masukkan nama yang sama untuk semua catatan dalam grup catatan tertimbang.

Untuk informasi selengkapnya tentang nama rekaman, lihat [Nama catatan](#)

Tipe catatan

Jenis data DNS. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Pilih nilai yang berlaku berdasarkan AWS sumber daya yang Anda rutekan lalu lintas ke:

API regional kustom API Gateway atau API yang dioptimalkan edge

Pilih A — IPv4 alamat.

Titik akhir antarmuka Amazon VPC

Pilih A — IPv4 alamat.

CloudFront distribusi

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi, buat dua catatan, satu dengan nilai A — IPv4 alamat untuk Jenis, dan satu dengan nilai AAAA — IPv6 alamat.

Layanan App Runner

Select A — IPv4 alamat

Lingkungan Elastic Beanstalk yang memiliki subdomain regional

Select A — IPv4 alamat

Penyeimbang beban ELB

Select A — IPv4 alamat atau AAAA — alamat IPv6

Buket Amazon S3

Select A — IPv4 alamat

OpenSearch Layanan

Select A — IPv4 alamat atau AAAA — alamat IPv6

Catatan lain di zona yang di-hosting ini

Pilih jenis catatan yang Anda buatkan alias. Semua jenis didukung kecuali NS dan SOA.

Note

Jika Anda membuat catatan alias yang memiliki nama yang sama sebagai zona yang di-hosting (dikenal sebagai zone apex), Anda tidak dapat merutekan lalu lintas ke catatan dengan nilai Jenis adalah CNAME. Ini karena catatan alias harus memiliki jenis yang sama dengan catatan yang Anda tuju, dan membuat catatan CNAME untuk Zone Apex tidak didukung bahkan untuk catatan alias.

Pilih nilai yang sama untuk semua catatan dalam kelompok grup tertimbang.

Nilai/Rutekan lalu lintas ke

Nilai yang Anda pilih dari daftar atau yang Anda ketik di bidang tergantung pada AWS sumber daya yang Anda rutekan lalu lintas.

Untuk informasi tentang AWS sumber daya yang dapat Anda targetkan, lihat [nilai umum untuk catatan alias untuk value/route lalu lintas](#).

Untuk informasi selengkapnya tentang cara mengonfigurasi Route 53 untuk merutekan lalu lintas ke AWS sumber daya tertentu, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Bobot

Nilai yang menentukan proporsi kueri DNS yang direspons Route 53 menggunakan catatan saat ini. Route 53 menghitung jumlah bobot untuk catatan yang memiliki kombinasi yang sama dari nama dan tipe DNS. Route 53 kemudian merespons kueri berdasarkan rasio bobot terhadap total milik sumber daya.

Anda tidak dapat membuat catatan tidak tertimbang yang memiliki nilai yang sama untuk Nama catatan dan Jenis catatan sebagai catatan tertimbang.

Masukkan bilangan bulat antara 0 dan 255. Untuk menonaktifkan perutean ke sumber daya, atur Bobot ke 0. Jika Anda menetapkan Bobot ke 0 untuk semua catatan dalam grup, lalu lintas dirutekan ke semua sumber daya dengan probabilitas yang sama. Hal ini memastikan bahwa Anda tidak secara tidak sengaja menonaktifkan perutean untuk grup catatan tertimbang.

Efek dari pengaturan Bobot ke 0 berbeda ketika Anda mengasosiasikan pemeriksaan kondisi dengan catatan tertimbang. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi](#).

Pemeriksaan kondisi

Pilih pemeriksaan kondisi jika Anda ingin Route 53 untuk memeriksa kondisi titik akhir tertentu dan untuk menanggapi permintaan DNS menggunakan catatan ini hanya ketika kondisi titik akhir baik.

Route 53 tidak memeriksa kondisi titik akhir yang ditentukan dalam catatan, misalnya, titik akhir yang ditentukan oleh alamat IP di bidang Nilai. Saat Anda memilih pemeriksaan kondisi untuk catatan, Route 53 memeriksa kondisi titik akhir yang Anda tentukan di pemeriksaan kondisi. Untuk informasi

tentang bagaimana Route 53 menentukan apakah titik akhir sehat, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Mengaitkan pemeriksaan kondisi dengan catatan hanya berguna ketika Route 53 memilih di antara dua catatan atau lebih untuk merespons kueri DNS, dan Anda ingin Route 53 mendasarkan pilihan sebagian pada status pemeriksaan kondisi. Gunakan pemeriksaan kondisi hanya dalam konfigurasi berikut:

- Anda sedang memeriksa kesehatan semua catatan dalam grup catatan yang memiliki nama, jenis, dan kebijakan perutean yang sama (seperti failover atau catatan tertimbang), dan Anda menentukan pemeriksaan kesehatan IDs untuk semua catatan. Jika pemeriksaan kondisi untuk catatan menentukan titik akhir yang tidak sehat, Route 53 berhenti merespons kueri menggunakan nilai untuk catatan tersebut.
- Anda memilih Ya untuk Mengevaluasi kesehatan target untuk catatan alias atau catatan dalam grup alias failover, alias geolokasi, alias latensi, alias berbasis IP, atau catatan alias tertimbang. Jika catatan alias mereferensikan catatan nonalias di zona yang dihosting yang sama, Anda juga harus menentukan pemeriksaan kesehatan untuk catatan yang direferensikan. Jika Anda mengaitkan pemeriksaan kesehatan dengan catatan alias dan juga memilih Ya untuk Evaluasi Kesehatan Target, keduanya harus mengevaluasi dengan benar. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

Jika pemeriksaan kondisi Anda menentukan titik akhir hanya berdasarkan nama domain, sebaiknya buat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`example.com`).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Mengevaluasi Kondisi Target

Pilih Ya jika Anda ingin Route 53 untuk menentukan apakah untuk menanggapi permintaan DNS menggunakan catatan ini dengan memeriksa kondisi sumber daya yang ditentukan oleh Titik akhir.

Perhatikan hal-hal berikut:

API Gateway khusus regional APIs dan dioptimalkan di tepi APIs

Tidak ada persyaratan khusus untuk menyetel Evaluasi kesehatan target ke Ya ketika titik akhir adalah API Regional kustom API Gateway API atau API yang dioptimalkan tepi.

CloudFront distribusi

Anda tidak dapat menetapkan Evaluasi kesehatan target ke Ya ketika titik akhir adalah CloudFront distribusi.

Lingkungan Elastic Beanstalk yang memiliki subdomain regionalisasi

Jika Anda menentukan lingkungan Elastic Beanstalk di Endpoint dan lingkungan berisi penyeimbang beban ELB, Elastic Load Balancing akan merutekan kueri hanya ke instans Amazon sehat yang terdaftar dengan penyeimbang beban. EC2 (Lingkungan secara otomatis berisi penyeimbang beban ELB jika menyertakan lebih dari satu EC2 instans Amazon.) Jika Anda menetapkan Evaluasi kesehatan target ke Ya dan tidak ada EC2 instans Amazon yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 mengarahkan kueri ke sumber daya lain yang tersedia yang sehat, jika ada.

Jika lingkungan berisi satu EC2 instance Amazon, tidak ada persyaratan khusus.

penyeimbang beban ELB

Perilaku pemeriksaan kondisi tergantung pada jenis penyeimbang beban:

- **Classic Load Balancers** — Jika Anda menentukan ELB Classic Load Balancer di Endpoint, Elastic Load Balancing akan merutekan kueri hanya ke instans EC2 Amazon sehat yang terdaftar dengan penyeimbang beban. Jika Anda menetapkan Evaluate Target Health ke Ya dan tidak ada EC2 instans yang sehat atau penyeimbang beban itu sendiri tidak sehat, Route 53 merutekan kueri ke sumber daya lain.
- **Aplikasi dan Penyeimbang Beban Jaringan** – Jika Anda menentukan Aplikasi ELB atau Penyeimbang Beban Jaringan dan Anda menyetel Evaluasi Kondisi Target ke Ya, Route 53 merutekan kueri ke penyeimbang beban berdasarkan kondisi grup target yang terkait dengan penyeimbang beban:
 - Agar Aplikasi atau Penyeimbang Beban Jaringan dianggap sehat, setiap kelompok target yang berisi target harus berisi setidaknya satu target yang sehat. Jika setiap kelompok target hanya berisi target yang tidak sehat, penyeimbang beban dianggap tidak sehat, dan Route 53 merutekan permintaan ke sumber daya lainnya.
 - Grup target yang tidak memiliki target terdaftar dianggap tidak sehat.

 Note

Bila Anda membuat penyeimbang beban, Anda mengonfigurasi pengaturan untuk pemeriksaan kondisi Elastic Load Balancing; bukan pemeriksaan kondisi Route 53, tetapi melakukan fungsi serupa. Jangan membuat pemeriksaan kesehatan Route 53 untuk EC2 kasus yang Anda daftarkan dengan penyeimbang beban ELB.

Bucket S3

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah bucket S3.

Titik akhir antarmuka Amazon VPC

Tidak ada persyaratan khusus untuk pengaturan Evaluasi kondisi target ke Ya ketika titik akhir adalah antarmuka Amazon VPC.

Catatan lain di zona yang di-hosting

Jika AWS sumber daya yang Anda tentukan di Endpoint adalah rekaman atau grup catatan (misalnya, grup catatan tertimbang) tetapi bukan catatan alias lain, sebaiknya Anda mengaitkan pemeriksaan kesehatan dengan semua catatan di titik akhir. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#).

ID catatan

Masukkan nilai yang secara unik mengidentifikasi catatan ini dalam grup catatan tertimbang.

Membuat catatan dengan mengimpor file zona

Jika Anda bermigrasi dari penyedia layanan DNS lain, dan jika penyedia layanan DNS Anda saat ini mengizinkan Anda mengekspor pengaturan DNS Anda saat ini ke file zona, Anda dapat dengan cepat membuat semua catatan untuk zona yang di-hosting Amazon Route 53 dengan mengimpor file zona.

 Note

File zona menggunakan format standar yang dikenal sebagai BIND untuk mewakili catatan dalam format teks. Untuk informasi tentang format file zona, lihat entri Wikipedia untuk [file](#)

[Zona](#). Informasi tambahan tersedia di [RFC 1034, Nama Domain—Konsep dan Fasilitas](#) bagian 3.6.1, dan [RFC 1035, Nama Domain—Implementasi dan Spesifikasi](#) bagian 5.

Jika Anda ingin membuat catatan dengan mengimpor file zona, perhatikan hal berikut:

- File zona harus dalam format yang sesuai dengan RFC.
- Nama domain catatan dalam file zona harus cocok dengan nama zona yang di-hosting.
- Route 53 mendukung kata kunci \$ORIGIN dan \$TTL. Jika file zona menyertakan kata kunci \$GENERATE atau \$INCLUDE, impor gagal dan Route 53 akan menghasilkan kesalahan.
- Saat Anda mengimpor file zona, Route 53 mengabaikan catatan SOA di file zona. Route 53 juga mengabaikan catatan NS yang memiliki nama yang sama sebagai zona yang di-hosting.
- Anda dapat mengimpor maksimum 1.000 catatan.
- Jika zona yang di-hosting sudah berisi catatan yang muncul di file zona, proses impor gagal, dan tidak ada catatan yang dibuat.
- Untuk catatan TXT yang berisi karakter garis miring terbalik, proses impor file zona menafsirkan urutan garis miring terbalik tertentu sebagai karakter kontrol. Untuk memasukkan karakter garis miring terbalik literal dalam nilai catatan TXT:
 - Gunakan garis miring terbalik ganda (\\) dalam file zona untuk mewakili garis miring terbalik literal tunggal dalam catatan TXT akhir.
 - Misalnya, jika catatan TXT Anda harus berisi \\jYTDWqH... (dengan garis miring terbalik literal dan j), tentukan \\\jYTDWqH... dalam file zona.

Ini sangat penting untuk catatan tantangan ACME dan catatan TXT lainnya yang berisi karakter garis miring terbalik literal.

- Untuk catatan TXT yang panjang (seperti catatan DKIM), proses impor file zona mendukung pemisahan konten menjadi beberapa string. Untuk membuat catatan TXT dengan beberapa string:
 - Gunakan baris terpisah di file zona Anda dengan nama dan jenis rekaman yang sama.

Example

```
example.com. 300 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC"
example.com. 300 IN TXT
    "7fCC6C13dM9tXuJmUBH7D4Vw8y1ByJ8z9QX2fvLm3pN4sR5tU6vW7xY8zA9bC0dE1f"
example.com. 300 IN TXT
    "G2hI3jK4lM5nO6pQ7rS8tU9vW0xY1zA2bC3dE4fG5hI6jK7lM8nO9pQ0rS1tU2vW3x"
```

Proses impor secara otomatis menggabungkan ini ke dalam satu catatan TXT dengan beberapa string. Setiap string individu dapat berisi hingga 65.535 karakter. Jangan menggabungkan string panjang menjadi satu nilai kutip.

- Kami menyarankan Anda meninjau konten file zona untuk mengonfirmasi bahwa nama catatan menyertakan atau mengecualikan titik beruntun yang sesuai:
 - Ketika nama catatan dalam file zona menyertakan titik beruntun (`example.com.`), proses impor menginterpretasikan nama sebagai nama domain yang memenuhi syarat dan menciptakan catatan Route 53 dengan nama tersebut.
 - Saat nama rekaman dalam file zona tidak menyertakan titik beruntun (`www`), proses impor menggabungkan nama tersebut dengan nama domain di file zona (`example.com`) dan membuat catatan Route 53 dengan nama gabungan (`www.example.com`).

Jika proses ekspor tidak menambahkan titik akhir ke nama domain yang sepenuhnya memenuhi syarat dari catatan, proses impor Route 53 menambahkan nama domain ke nama catatan. Misalnya, anggap Anda mengimpor data ke zona yang di-hosting `example.com` dan nama catatan MX dalam file zona adalah `mail.example.com`, tanpa titik beruntun. Proses impor Route 53 menciptakan catatan MX bernama `mail.example.com.example.com`.

Important

Untuk data CNAME, MX, PTR, dan SRV, perilaku ini juga berlaku untuk nama domain yang disertakan dalam nilai RDATA. Misalnya, anggap Anda memiliki file zona untuk `example.com`. Jika data CNAME dalam file zona (`support`, tanpa titik beruntun) memiliki nilai RDATA `www.example.com` (juga tanpa titik beruntun), proses impor membuat catatan Route 53 dengan nama `support.example.com` yang merutekan lalu lintas ke `www.example.com.example.com`. Sebelum Anda mengimpor file zona Anda, tinjau nilai RDATA dan perbarui sebagaimana berlaku. Untuk catatan TXT yang berisi karakter garis miring terbalik, gunakan garis miring terbalik ganda (`\\\\`) di file zona untuk mewakili garis miring terbalik literal.

Route 53 tidak mendukung mengekspor catatan ke file zona.

 Note

Jika Anda membuat catatan yang memiliki nama yang sama dengan zona yang di-hosting, jangan masukkan nilai (misalnya, simbol @) di bidang Nama.

Untuk membuat catatan dengan mengimpor file zona

1. Dapatkan file zona dari penyedia layanan DNS yang saat ini melayani domain. Proses dan terminologi bervariasi dari satu penyedia layanan ke yang lain. Lihat antarmuka dan dokumentasi penyedia Anda untuk informasi tentang mengekspor atau menyimpan catatan Anda dalam file zona atau file BIND.

Jika prosesnya tidak jelas, coba tanyakan dukungan pelanggan penyedia DNS Anda saat ini untuk daftar catatan atau informasi file zona.

2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Hosted zones (Zona yang di-hosting).
4. Pada halaman Zona yang Di-hosting, buat zona yang di-hosting baru:
 - a. Pilih Create hosted zone (Buat Zona yang Di-hosting).
 - b. Masukkan nama domain Anda dan, secara opsional, memberikan komentar.
 - c. Pilih Buat.
5. Pilih Import zone file (Impor file zona).
6. Di panel Import zone file (Impor file zona), tempel isi dari file zona Anda ke kotak teks Zone file (File zona).
7. Pilih Import (Impor).

 Note

Bergantung pada jumlah rekaman dalam file zona Anda, Anda mungkin harus menunggu beberapa menit hingga catatan dibuat.

8. Jika Anda menggunakan layanan DNS lain untuk domain tersebut (yang biasa terjadi jika Anda mendaftarkan domain dengan registrar lain), migrasikan layanan DNS ke Route 53. Ketika langkah itu selesai, pencatat Anda akan mulai mengidentifikasi Route 53 sebagai layanan DNS

Anda sebagai tanggapan atas kueri DNS untuk domain Anda, dan kueri akan mulai dikirim ke server DNS Route 53. (Biasanya, ada satu atau dua hari penundaan sebelum kueri DNS mulai dirutekan ke Route 53 karena informasi tentang layanan DNS Anda sebelumnya di-cache pada DNS resolver selama itu.) Untuk informasi selengkapnya, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengedit catatan

Prosedur berikut menjelaskan cara mengedit catatan menggunakan konsol Amazon Route 53. Untuk informasi tentang cara mengedit rekaman menggunakan API Route 53, lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.

Note

Perubahan untuk catatan membutuhkan waktu untuk menyebarkan ke server DNS Route 53. Saat ini, satu-satunya cara untuk memverifikasi bahwa perubahan telah disebarkan adalah dengan menggunakan tindakan [GetChange](#) API. Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Untuk mengedit catatan menggunakan konsol Route 53

1. Jika Anda tidak mengedit catatan alias, lewati ke langkah 2.

Jika Anda mengedit catatan alias yang merutekan lalu lintas ke Elastic Load Balancing Classic Load Balancer, Application Load Balancer, atau Network Load Balancer, dan jika Anda membuat zona host Route 53 dan penyeimbang beban Anda menggunakan akun yang berbeda, [Mendapatkan nama DNS untuk penyeimbang beban Elastic Load Balancing](#) lakukan prosedur untuk mendapatkan nama DNS untuk penyeimbang beban.

Jika Anda mengedit catatan alias untuk AWS sumber daya lain, lewati ke langkah 2.

2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Hosted zones (Zona yang di-hosting).
4. Di halaman Hosted Zones (Zona yang Di-hosting), pilih baris untuk zona yang di-hosting tempat Anda ingin mengedit catatan.

5. Pilih baris untuk rekaman yang ingin Anda edit, lalu masukkan perubahan Anda di panel Edit catatan.
6. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau mengedit catatan Amazon Route 53](#).
7. Pilih Save changes (Simpan perubahan).
8. Jika Anda mengedit beberapa catatan, ulangi langkah 5 hingga 7.

Menghapus catatan

Prosedur berikut menjelaskan cara menghapus catatan menggunakan konsol Route 53. Untuk informasi tentang cara menghapus rekaman menggunakan API Route 53, lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.

Note

Perubahan untuk catatan membutuhkan waktu untuk menyebarkan ke server DNS Route 53. Saat ini, satu-satunya cara untuk memverifikasi bahwa perubahan telah disebarkan adalah dengan menggunakan tindakan [GetChangeAPI](#). Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Membatalkan catatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di halaman Zona yang Di-hosting, pilih baris untuk zona yang di-hosting tempat Anda ingin menghapus catatan.
3. Dalam daftar catatan, pilih data yang ingin Anda hapus.

Untuk memilih beberapa catatan berturut-turut, pilih baris pertama, tahan tombol Shift, dan pilih baris terakhir. Untuk memilih beberapa catatan yang tidak berurutan, pilih baris pertama, tahan tombol Ctrl, dan pilih baris tambahan.

Anda tidak dapat menghapus catatan yang memiliki nilai NS atau SOA untuk Jenis.

4. Pilih Delete (Hapus).
5. Pilih Delete (Hapus) untuk menutup kotak dialog.

Mencantumkan catatan

Prosedur berikut menjelaskan cara menggunakan konsol Amazon Route 53 untuk daftar catatan di zona yang di-hosting. Untuk informasi tentang cara mencantumkan catatan menggunakan API Route 53, lihat [ListResourceRecordSets](#) di Referensi API Amazon Route 53.

Untuk mencantumkan catatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pada halaman Zona yang Di-hosting, pilih nama zona yang di-hosting.
4. Untuk mengubah mode pencarian, pilih ikon roda gigi di kanan atas tabel Rekaman. Pilih salah satu dari:

- Otomatis

Dalam mode ini, layanan menggunakan filter berdasarkan sejumlah catatan. Penuh kurang dari 2000 dan cepat untuk lebih dari 2000 catatan.

- Penuh

Dalam mode ini, semua filter pencarian tersedia, tetapi kinerja pencarian mungkin lebih lambat.

- Cepat

Dalam mode ini, beberapa fitur canggih tidak tersedia, tetapi kinerja pencarian akan lebih cepat.

Untuk hanya menampilkan catatan yang dipilih, masukkan kriteria pencarian yang berlaku di atas daftar catatan. Dalam mode otomatis, perilaku pencarian bergantung pada apakah zona yang dihosting berisi hingga 2.000 catatan atau lebih dari 2.000 catatan:

Hingga 2.000 catatan dan mode penuh

- Untuk menampilkan catatan yang memiliki nilai tertentu, masukkan nilai di bilah pencarian dan tekan Enter. Misalnya, untuk menampilkan catatan yang memiliki alamat IP yang dimulai dengan 192.0, masukkan nilai tersebut di bidang Search (Pencarian), dan tekan Enter.

- Untuk menampilkan hanya catatan yang memiliki jenis data DNS yang sama, pilih Jenis catatan dalam daftar menurun, dan masukkan jenis catatan.
- Untuk hanya menampilkan catatan alias, pilih Alias di daftar dropdown, dan masukkan. **Yes**
- Untuk hanya menampilkan catatan tertimbang, pilih Kebijakan perutean dalam daftar menurun, dan masukkan **WEIGHTED**.

Lebih dari 2.000 catatan dan mode cepat

- Anda dapat mencari hanya pada nama catatan, bukan pada nilai catatan. Anda juga tidak dapat memfilter berdasarkan jenis catatan, atau pada alias atau catatan tertimbang.

Untuk melakukan ini, masukkan kursor Anda ke kotak teks Filter, pilih Properti dan kemudian Rekam nama.

- Untuk catatan yang memiliki tiga label (tiga bagian dipisahkan oleh titik), ketika Anda memasukkan nilai di kolom pencarian dan menekan Enter, konsol Route 53 secara otomatis melakukan pencarian wildcard pada label ketiga dari kanan dalam nama catatan. Misalnya, zona yang di-hosting example.com berisi 100 catatan bernama record1.example.com melalui record100.example.com. (Record1 adalah label ketiga dari kanan.) Inilah yang terjadi saat Anda mencari nilai berikut:
 - record1 – Konsol Route 53 mencari record1*.example.com, yang akan menghasilkan record1.example.com, record10.example.com melalui record19.example.com, dan record100.example.com.
 - record1.example.com – Seperti pada contoh sebelumnya, konsol akan melakukan pencarian untuk record1*.example.com dan menghasilkan catatan yang sama.
 - 1 – Konsol melakukan pencarian untuk 1*.example.com dan tidak menghasilkan catatan.
 - Example – Konsol melakukan pencarian untuk example*.example.com dan tidak menghasilkan catatan.
 - example.com – Dalam contoh ini, konsol tidak melakukan pencarian wildcard. Hal ini akan menghasilkan semua catatan di zona yang di-hosting.
 - Mode pencarian otomatis — Saat menggunakan mode pencarian ini, Anda harus terlebih dahulu menyediakan properti, seperti nama rekam, untuk dapat mencari.

Note

Jika label ketiga dari kanan berisi satu atau lebih tanda hubung (seperti `third-label.example.com`), dan jika Anda mencari bagian dari label ketiga tepat sebelum tanda hubung (`third` dalam contoh ini), Route 53 tidak akan menghasilkan catatan

apa pun. Sebagai gantinya, sertakan tanda hubung (cari `third-`) atau hilangkan karakter segera sebelum tanda hubung (cari `third`).

- Untuk catatan yang memiliki empat label atau lebih, Anda harus menentukan nama yang tepat dari catatan. Tidak ada pencarian wildcard yang didukung. Sebagai contoh, jika zona yang di-hosting menyertakan catatan bernama `label4.record1.example.com`, Anda dapat menemukan catatan itu hanya jika Anda menentukan `label4.record1.example.com` di bidang pencarian.

Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53

Penandatanganan Domain Name System Security Extensions (DNSSEC) memungkinkan penyelesaian DNS memvalidasi bahwa respons DNS berasal dari Amazon Route 53 dan belum diubah. Ketika Anda menggunakan penandatanganan DNSSEC, setiap respons untuk zona yang di-hosting ditandatangani menggunakan kriptografi kunci publik. Untuk ikhtisar DNSSEC, lihat bagian DNSSEC dari [AWS re:Invent 2021 - Amazon Route 53](#): Setahun dalam peninjauan.

Dalam Bab ini, kami menjelaskan cara mengaktifkan penandatanganan DNSSEC untuk Route 53, cara bekerja dengan kunci penandatanganan kunci (KSKs), dan cara memecahkan masalah. Anda dapat bekerja dengan penandatanganan DNSSEC Konsol Manajemen AWS atau secara terprogram dengan API. Untuk informasi lebih lanjut tentang menggunakan CLI atau SDKs untuk bekerja dengan Route 53, lihat [Siapkan Amazon Route 53](#).

Sebelum Anda mengaktifkan penandatanganan DNSSEC, perhatikan hal berikut:

- Untuk membantu mencegah pemadaman zona dan menghindari masalah dengan domain yang menjadi tidak tersedia, Anda harus cepat mengatasi dan menyelesaikan kesalahan DNSSEC. Kami sangat menyarankan agar Anda mengatur CloudWatch alarm yang memberi tahu Anda setiap kali `DNSSECKeySigningKeysNeedingAction` kesalahan `DNSSECInternalFailure` atau terdeteksi. Untuk informasi selengkapnya, lihat [Memantau zona yang dihosting menggunakan Amazon CloudWatch](#).
- Ada dua jenis kunci dalam DNSSEC: kunci penandatanganan kunci (KSK) dan kunci penandatanganan zona (ZSK). Dalam penandatanganan DNSSEC Route 53, setiap KSK didasarkan pada [kunci yang dikelola pelanggan asimetris](#) yang Anda miliki. AWS KMS Anda bertanggung jawab atas manajemen KSK, yang mencakup rotasi jika diperlukan. Manajemen ZSK dilakukan oleh Route 53.
- Jika Anda mengaktifkan penandatanganan DNSSEC untuk zona yang di-hosting, Route 53 membatasi TTL menjadi satu minggu. Jika Anda menetapkan TTL lebih dari satu minggu untuk

catatan di zona yang di-hosting, Anda tidak akan mendapatkan kesalahan. Namun, Route 53 memberlakukan TTL selama satu minggu untuk catatan. Catatan yang memiliki TTL kurang dari satu minggu dan catatan di zona yang di-hosting lain dengan penandatanganan DNSSEC yang dinonaktifkan tidak akan terpengaruh.

- Ketika Anda menggunakan penandatanganan DNSSEC, konfigurasi multi-vendor tidak didukung. Jika Anda telah mengonfigurasi server nama label putih (juga dikenal sebagai server nama vanity atau server nama pribadi), pastikan server nama tersebut disediakan oleh penyedia DNS tunggal.
- Beberapa penyedia DNS tidak mendukung catatan Delegation Signer (DS) dalam DNS otoritatif mereka. Jika zona induk Anda di-host oleh penyedia DNS yang tidak mendukung kueri DS (tidak menyetel tanda AA dalam respons kueri DS), maka saat Anda mengaktifkan DNSSEC di zona turunannya, zona anak akan menjadi tidak dapat diselesaikan. Pastikan penyedia DNS Anda mendukung catatan DS.
- Hal ini dapat membantu untuk menyiapkan izin IAM guna mengizinkan pengguna lain, selain pemilik zona, untuk menambah atau menghapus catatan di zona. Sebagai contoh, pemilik zona dapat menambahkan KSK dan mengaktifkan penandatanganan, dan mungkin juga bertanggung jawab atas rotasi kunci. Namun, orang lain mungkin bertanggung jawab untuk bekerja dengan catatan lain pada zona yang di-hosting. Untuk contoh kebijakan IAM, lihat [Contoh izin untuk pemilik catatan domain](#).
- Untuk memeriksa apakah TLD memiliki dukungan DNSSEC, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Topik

- [Mengaktifkan penandatanganan DNSSEC dan membuat rantai kepercayaan](#)
- [Menonaktifkan penandatanganan DNSSEC](#)
- [Bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC](#)
- [Bekerja dengan kunci penandatanganan kunci \(\) KSKs](#)
- [Kunci KMS dan manajemen ZSK di Route 53](#)
- [Bukti DNSSEC tentang ketidakberadaan di Route 53](#)
- [Memecahkan masalah penandatanganan DNSSEC](#)

Mengaktifkan penandatanganan DNSSEC dan membuat rantai kepercayaan

Langkah-langkah tambahan berlaku untuk pemilik zona yang dihosting dan pengelola zona induk. Ini bisa menjadi orang yang sama, tetapi jika tidak, pemilik zona harus memberi tahu dan bekerja dengan pengelola zona induk.

Kami merekomendasikan mengikuti langkah-langkah dalam artikel ini agar zona Anda ditandatangani dan dimasukkan dalam rantai kepercayaan. Langkah-langkah berikut akan meminimalkan risiko orientasi ke DNSSEC.

Note

Pastikan Anda membaca prasyarat sebelum memulai. [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#)

Ada tiga langkah yang harus diambil untuk mengaktifkan penandatanganan DNSSEC, seperti yang dijelaskan di bagian berikut.

Topik

- [Langkah 1: Bersiaplah untuk mengaktifkan penandatanganan DNSSEC](#)
- [Langkah 2: Aktifkan penandatanganan DNSSEC dan buat KSK](#)
- [Langkah 3: Membangun rantai kepercayaan](#)

Langkah 1: Bersiaplah untuk mengaktifkan penandatanganan DNSSEC

Langkah-langkah persiapan membantu Anda meminimalkan risiko orientasi ke DNSSEC dengan memantau ketersediaan zona dan menurunkan waktu tunggu antara mengaktifkan penandatanganan dan penyisipan catatan Penandatanganan Delegasi (DS).

Untuk mempersiapkan untuk mengaktifkan penandatanganan DNSSEC

1. Pantau ketersediaan zona.

Anda dapat memantau zona untuk ketersediaan nama domain Anda. Ini dapat membantu Anda mengatasi masalah apa pun yang mungkin memerlukan mundur selangkah setelah Anda mengaktifkan penandatanganan DNSSEC. Anda dapat memantau nama domain Anda

dengan sebagian besar lalu lintas dengan menggunakan pencatatan kueri. Untuk informasi selengkapnya tentang menyiapkan pencatatan kueri, lihat [Memantau Amazon Route 53](#).

Pemantauan dapat dilakukan melalui skrip shell, atau melalui layanan pihak ketiga. Namun, seharusnya tidak menjadi satu-satunya sinyal untuk menentukan apakah rollback diperlukan. Anda mungkin juga mendapatkan umpan balik dari pelanggan Anda karena domain tidak tersedia.

2. Turunkan TTL maksimum zona.

TTL maksimum zona adalah rekor TTL terpanjang di zona tersebut. Di zona contoh berikut, TTL maksimum zona adalah 1 hari (86400 detik).

Nama	TTL	Kelas rekam	Tipe catatan	Rekam data
example.com.	900	DI DALAM	SOA	ns1.example.com. hostmaster.example.com. 200202240 1 10800 15 604800 300
example.com.	900	DI DALAM	NS	ns1.example.com.
route53.example.com.	86400	DI DALAM	TXT	some txt record

Menurunkan TTL maksimum zona akan membantu mengurangi waktu tunggu antara mengaktifkan penandatanganan dan penyisipan catatan Penandatanganan Delegasi (DS). Kami merekomendasikan untuk menurunkan TTL maksimum zona menjadi 1 jam (3600 detik). Ini memungkinkan Anda untuk memutar kembali setelah hanya satu jam jika ada penyelesaian yang memiliki masalah dengan catatan yang ditandatangani caching.

Rollback: batalkan perubahan TTL.

3. Turunkan bidang minimum SOA TTL dan SOA.

Bidang minimum SOA adalah bidang terakhir dalam data catatan SOA. Dalam contoh berikut catatan SOA, bidang minimum memiliki nilai 5 menit (300 detik).

Nama	TTL	Kelas rekam	Tipe catatan	Rekam data
example.com.	900	DI DALAM	SOA	ns1.example.com. hostmaster.example.com. 200202240 1 10800 15 604800 300

Bidang minimum SOA TTL dan SOA menentukan berapa lama resolver mengingat jawaban negatif. Setelah Anda mengaktifkan penandatanganan, server nama Route 53 mulai mengembalikan catatan NSEC untuk jawaban negatif. NSEC berisi informasi yang mungkin digunakan resolver untuk mensintesis jawaban negatif. Jika Anda harus memutar kembali karena informasi NSEC menyebabkan resolver mengasumsikan jawaban negatif untuk sebuah nama, maka Anda hanya perlu menunggu maksimum bidang minimum SOA TTL dan SOA agar resolver menghentikan asumsi.

Rollback: batalkan perubahan SOA.

4. Pastikan perubahan bidang minimum TTL dan SOA efektif.

Gunakan [GetChange](#) untuk memastikan perubahan Anda sejauh ini telah disebarkan ke semua server DNS Route 53.

Langkah 2: Aktifkan penandatanganan DNSSEC dan buat KSK

Anda dapat mengaktifkan penandatanganan DNSSEC dan membuat kunci penandatanganan kunci (KSK) dengan menggunakan AWS CLI atau di konsol Route 53.

- [CLI](#)
- [Konsol](#)

Saat Anda memberikan atau membuat kunci KMS, ada beberapa persyaratan. Untuk informasi selengkapnya, lihat [Bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC](#).

CLI

Anda dapat menggunakan kunci yang sudah Anda miliki, atau membuatnya dengan menjalankan AWS CLI perintah seperti berikut menggunakan nilai Anda sendiri untuk `hostedzone_id`, `cmk_arn`, `ksk_name`, dan `unique_string` (untuk membuat permintaan unik):

```
aws --region us-east-1 route53 create-key-signing-key \
  --hosted-zone-id $hostedzone_id \
  --key-management-service-arn $cmk_arn --name $ksk_name \
  --status ACTIVE \
  --caller-reference $unique_string
```

Untuk informasi selengkapnya tentang kunci yang dikelola pelanggan, lihat [Bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC](#). Lihat juga [CreateKeySigningKey](#).

Untuk mengaktifkan penandatanganan DNSSEC, jalankan AWS CLI perintah seperti berikut, menggunakan nilai Anda sendiri untuk: `hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
  --hosted-zone-id $hostedzone_id
```

Untuk informasi lebih lanjut, lihat [enable-hosted-zone-dnssec](#) dan [EnableHostedZoneDNSSEC](#).

Console

Cara mengaktifkan penandatanganan DNSSEC dan membuat KSK

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih zona yang di-hosting, lalu pilih zona yang di-hosting dengan penandatanganan DNSSEC yang ingin Anda aktifkan.
3. Di tab Penandatanganan DNSSEC, pilih Aktifkan penandatanganan DNSSEC.

Note

Jika opsi di bagian ini adalah Nonaktifkan penandatanganan DNSSEC, Anda telah menyelesaikan langkah pertama dalam mengaktifkan penandatanganan DNSSEC.

Pastikan bahwa Anda membuat, atau sudah ada, rantai kepercayaan bagi zona yang di-hosting untuk DNSSEC, lalu Anda selesai. Untuk informasi selengkapnya, lihat [Langkah 3: Membangun rantai kepercayaan](#).

4. Di bagian pembuatan Kunci Penandatanganan Kunci (KSK), pilih Buat KSK baru, dan di bawah Berikan nama KSK, masukkan nama untuk KSK yang akan dibuat Route 53 untuk Anda. Nama dapat mencakup angka, huruf, dan garis bawah (_). Nama ini harus unik.
5. Di bawah CMK yang dikelola Pelanggan, pilih kunci terkelola pelanggan untuk Route 53 untuk digunakan saat membuat KSK untuk Anda. Anda dapat menggunakan kunci terkelola pelanggan yang sudah ada yang berlaku untuk penandatanganan DNSSEC, atau membuat kunci terkelola pelanggan baru.

Saat Anda memberikan atau membuat kunci yang dikelola pelanggan, ada beberapa persyaratan. Untuk informasi selengkapnya, lihat [Bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC](#).

6. Masukkan alias untuk kunci terkelola pelanggan yang sudah ada. Jika Anda ingin menggunakan kunci terkelola pelanggan baru, masukkan alias untuk kunci yang dikelola pelanggan, dan Route 53 akan membuatnya untuk Anda.

 Note

Jika Anda memilih agar Route 53 membuat kunci terkelola pelanggan, ketahuilah bahwa biaya terpisah berlaku untuk setiap kunci yang dikelola pelanggan. Untuk informasi selengkapnya, lihat [Harga Layanan Manajemen Kunci AWS](#).

7. Pilih Aktifkan penandatanganan DNSSEC.

Setelah Anda mengaktifkan penandatanganan zona, selesaikan langkah-langkah berikut (apakah Anda menggunakan konsol atau CLI):

1. Pastikan penandatanganan zona efektif.

Jika digunakan AWS CLI, Anda dapat menggunakan Id operasi dari output `EnableHostedZoneDNSSEC()` panggilan untuk menjalankan [get-change](#) atau [GetChange](#) untuk memastikan bahwa semua Server DNS Route 53 menandatangani tanggapan (status =). INSYNC

2. Tunggu setidaknya TTL maksimum zona sebelumnya.

Tunggu resolver untuk menghapus semua catatan yang tidak ditandatangani dari cache mereka. Untuk mencapai ini, Anda harus menunggu setidaknya TTL maksimum zona sebelumnya. Di `example.com` zona di atas, waktu tunggu adalah 1 hari.

3. Memantau laporan masalah pelanggan.

Setelah Anda mengaktifkan penandatanganan zona, pelanggan Anda mungkin mulai melihat masalah yang terkait dengan perangkat jaringan dan resolver. Periode pemantauan yang disarankan adalah 2 minggu.

Berikut ini adalah contoh masalah yang mungkin Anda lihat:

- Beberapa perangkat jaringan dapat membatasi ukuran respons DNS hingga di bawah 512 byte, yang terlalu kecil untuk beberapa respons yang ditandatangani. Perangkat jaringan ini harus dikonfigurasi ulang untuk memungkinkan ukuran respons DNS yang lebih besar.
- Beberapa perangkat jaringan melakukan inspeksi mendalam pada respons DNS dan menghapus catatan tertentu yang tidak dimengerti, seperti yang digunakan untuk DNSSEC. Perangkat ini harus dikonfigurasi ulang.
- Beberapa resolver pelanggan mengklaim bahwa mereka dapat menerima respons UDP yang lebih besar daripada dukungan jaringan mereka. Anda dapat menguji kemampuan jaringan Anda dan mengonfigurasi resolver Anda dengan tepat. Untuk informasi selengkapnya lihat, [DNS Reply Size Test Server](#).

Rollback: panggil [DisableHostedZoneDNSSEC](#) lalu kembalikan langkah-langkahnya. [Langkah 1: Bersiaplah untuk mengaktifkan penandatanganan DNSSEC](#)

Langkah 3: Membangun rantai kepercayaan

Setelah Anda mengaktifkan penandatanganan DNSSEC untuk zona yang di-hosting di Route 53, buat rantai kepercayaan untuk zona yang di-hosting guna menyelesaikan penyiapan penandatanganan DNSSEC. Anda melakukan ini dengan membuat catatan Delegation Signer (DS) di zona yang di-hosting induk, untuk zona yang di-hosting, menggunakan informasi yang disediakan Route 53. Tergantung pada tempat domain terdaftar, Anda menambahkan catatan ke zona yang di-hosting induk di Route 53 atau registrar domain lain.

Cara membuat rantai kepercayaan untuk penandatanganan DNSSEC

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

2. Di panel navigasi, pilih zona yang di-hosting, lalu pilih zona yang di-hosting yang ingin dibuatkan rantai kepercayaan DNSSEC. Anda harus mengaktifkan penandatanganan DNSSEC terlebih dahulu.
3. Di tab Penandatanganan DNSSEC, di bawah Penandatanganan DNSSEC, pilih Lihat informasi untuk membuat catatan DS.

 Note

Jika tidak melihat Lihat informasi untuk membuat catatan DS di bagian ini, Anda harus mengaktifkan penandatanganan DNSSEC sebelum membuat rantai kepercayaan. Pilih Aktifkan penandatanganan DNSSEC dan selesaikan langkah-langkah seperti yang dijelaskan [Langkah 2: Aktifkan penandatanganan DNSSEC dan buat KSK](#), lalu kembali ke langkah-langkah ini untuk membangun rantai kepercayaan.

4. Di bawah Buat rantai kepercayaan, pilih salah satu Registrar Route 53 atau Registrar domain lainnya, tergantung tempat domain Anda terdaftar.
5. Gunakan nilai yang disediakan dari langkah 3 untuk membuat catatan DS untuk zona host induk di Route 53. Jika domain Anda tidak di-host di Route 53, gunakan nilai yang disediakan untuk membuat catatan DS di situs web registrar domain Anda.

Membangun rantai kepercayaan untuk zona induk:

- Jika domain Anda dikelola melalui Route 53, ikuti langkah-langkah berikut:

Pastikan Anda mengonfigurasi algoritma penandatanganan yang benar (ECDSAP256SHA256 dan ketik 13) dan algoritma intisari (SHA-256 dan tipe 2).

Jika Route 53 adalah registrar Anda, lakukan hal berikut di konsol Route 53:

1. Catat nilai Jenis kunci, Algoritme, dan Kunci publik. Di panel navigasi, pilih Domain terdaftar.
2. Pilih domain, dan kemudian, dalam tab kunci DNSSEC, pilih Tambah kunci.
3. Dalam kotak dialog Kelola kunci DNSSEC, pilih jenis Kunci dan Algoritma yang sesuai untuk registrar Route 53 dari menu tarik-turun.
4. Salin Kunci publik untuk registrar Route 53. Di kotak dialog Kelola kunci DNSSEC, tempelkan nilainya ke kotak kunci Publik.
5. Pilih Tambahkan.

Route 53 akan menambahkan catatan DS ke zona induk dari kunci publik. Misalnya, jika domain Anda `example.com`, catatan DS ditambahkan ke zona `DNS.com`.

- Jika domain Anda dikelola di registri lain, ikuti instruksi di bagian Registrar domain lain.

Untuk memastikan langkah-langkah berikut berjalan lancar, perkenalkan DS TTL rendah ke zona induk. Kami merekomendasikan pengaturan DS TTL ke 5 menit (300 detik) untuk pemulihan yang lebih cepat jika Anda perlu mengembalikan perubahan Anda.

- Membangun rantai kepercayaan untuk zona anak:

Jika zona induk Anda dikelola oleh registri lain, hubungi registrar Anda untuk memperkenalkan catatan DS untuk zona Anda. Biasanya Anda tidak akan dapat menyesuaikan TTL dari catatan DS.

- Jika zona induk Anda di-host di Route 53, hubungi pemilik zona induk untuk memperkenalkan catatan DS untuk zona Anda.

Berikan `$ds_record_value` kepada pemilik zona induk. Anda bisa mendapatkannya dengan mengklik Lihat Informasi untuk membuat catatan DS di konsol dan menyalin bidang catatan DS, atau dengan memanggil [GetDNSSEC](#) API dan mengambil nilai bidang `"DSRecord"`

```
aws --region us-east-1 route53 get-dnssec
    --hosted-zone-id $hostedzone_id
```

Pemilik zona induk dapat memasukkan catatan melalui konsol Route 53 atau CLI.

- Untuk menyisipkan catatan DS dengan menggunakan AWS CLI, pemilik zona induk membuat dan memberi nama file JSON yang mirip dengan contoh berikut. Pemilik zona induk mungkin memberi nama file seperti `inserting_ds.json`.

```
{
  "HostedZoneId": "$parent_zone_id",
  "ChangeBatch": {
    "Comment": "Inserting DS for zone $zone_name",
    "Changes": [
      {
        "Action": "UPSERT",
        "ResourceRecordSet": {
          "Name": "$zone_name",
          "Type": "DS",
```

```

        "TTL": 300,
        "ResourceRecords": [
            {
                "Value": "$ds_record_value"
            }
        ]
    }
}

```

Kemudian jalankan perintah berikut:

```

aws --region us-east-1 route53 change-resource-record-sets
    --cli-input-json file://inserting_ds.json

```

- Untuk memasukkan catatan DS dengan menggunakan konsol,

Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Di panel navigasi, pilih Zona yang dihosting, nama zona yang dihosting, lalu tombol Buat rekam. Pastikan Anda memilih Perutean sederhana untuk kebijakan Routing.

Di bidang Nama rekam masukkan nama yang sama dengan \$zone_name, pilih DS dari jenis Rekam tarik-turun, dan masukkan nilai \$ds_record_value ke dalam bidang Nilai, dan pilih Buat catatan.

Rollback: hapus DS dari zona induk, tunggu DS TTL, lalu putar kembali langkah-langkah untuk membangun kepercayaan. Jika zona induk di-host di Route 53, pemilik zona induk dapat mengubah Action dari UPSERT ke DELETE dalam file JSON, dan menjalankan kembali contoh CLI di atas.

6. Tunggu pembaruan disebar, berdasarkan TTL untuk catatan domain Anda.

Jika zona induk ada di layanan DNS Route 53, pemilik zona induk dapat mengonfirmasi propagasi penuh melalui API. [GetChange](#)

Jika tidak, Anda dapat secara berkala menyelidiki zona induk untuk catatan DS, dan kemudian menunggu 10 menit setelahnya untuk meningkatkan kemungkinan penyisipan catatan DS

disebarkan sepenuhnya. Perhatikan bahwa beberapa pendaftar telah menjadwalkan penyisipan DS, misalnya, sekali sehari.

Saat Anda memperkenalkan catatan Penandatanganan Delegasi (DS) di zona induk, resolver tervalidasi yang telah mengambil DS akan mulai memvalidasi tanggapan dari zona tersebut.

Untuk memastikan langkah-langkah membangun kepercayaan berjalan lancar, selesaikan hal-hal berikut:

1. Temukan NS TTL maksimum.

Ada 2 set catatan NS yang terkait dengan zona Anda:

- Catatan NS delegasi — ini adalah catatan NS untuk zona Anda yang dipegang oleh zona induk. Anda dapat menemukannya dengan menjalankan perintah Unix berikut (jika zona Anda adalah example.com, zona induknya adalah com):

```
dig -t NS com
```

Pilih salah satu catatan NS dan kemudian jalankan yang berikut ini:

```
dig @one of the NS records of your parent zone -t NS example.com
```

Contoh:

```
dig @b.gtld-servers.net. -t NS example.com
```

- Catatan NS dalam zona — ini adalah catatan NS di zona Anda. Anda dapat menemukan ini dengan menjalankan perintah Unix berikut:

```
dig @one of the NS records of your zone -t NS example.com
```

Contoh:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

Perhatikan TTL maksimum untuk kedua zona.

2. Tunggu NS TTL maksimum.

Sebelum penyisipan DS, resolver mendapatkan respons yang ditandatangani, tetapi tidak memvalidasi tanda tangan. Ketika catatan DS dimasukkan, resolver tidak akan melihatnya

sampai catatan NS untuk zona berakhir. Ketika resolver mengambil kembali catatan NS, catatan DS kemudian akan dikembalikan.

Jika pelanggan Anda menjalankan resolver pada host dengan jam yang tidak sinkron, pastikan jam berada dalam 1 jam dari waktu yang benar.

Setelah menyelesaikan langkah ini, semua resolver yang sadar DNSSEC akan memvalidasi zona Anda.

3. Amati resolusi nama.

Anda harus memperhatikan bahwa tidak ada masalah dengan resolver yang memvalidasi zona Anda. Pastikan Anda juga memperhitungkan waktu yang dibutuhkan pelanggan Anda untuk melaporkan masalah kepada Anda.

Kami merekomendasikan pemantauan hingga 2 minggu.

4. (Opsional) Perpanjang DS dan NS TTLs.

Jika Anda puas dengan pengaturan, Anda dapat menyimpan perubahan TTL dan SOA yang Anda buat. Perhatikan bahwa Route 53 membatasi TTL hingga 1 minggu untuk zona yang ditandatangani. Untuk informasi selengkapnya, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

Jika Anda dapat mengubah DS TTL, kami sarankan Anda mengaturnya ke 1 jam.

Menonaktifkan penandatanganan DNSSEC

Langkah untuk menonaktifkan penandatanganan DNSSEC Route 53 dapat beragam, tergantung pada rantai kepercayaan yang menjadi bagian dari zona yang di-hosting.

Misalnya, zona yang di-hosting Anda mungkin memiliki zona induk yang memiliki catatan Delegation Signer (DS), sebagai bagian dari rantai kepercayaan. Zona yang di-hosting mungkin juga adalah zona induk untuk zona anak yang telah mengaktifkan penandatanganan DNSSEC, yang merupakan bagian lain dari rantai kepercayaan. Selidiki dan tentukan rantai kepercayaan penuh untuk zona yang di-hosting sebelum Anda mengambil langkah untuk menonaktifkan penandatanganan DNSSEC.

Rantai kepercayaan untuk zona yang di-hosting yang mengizinkan penandatanganan DNSSEC harus dibatalkan secara hati-hati saat Anda menonaktifkan penandatanganan. Untuk menghapus zona yang di-hosting dari rantai kepercayaan, Anda menghapus semua catatan DS yang ada untuk

rantai kepercayaan yang mencakup zona yang di-hosting ini. Ini berarti Anda harus melakukan hal berikut, agar dapat:

1. Menghapus catatan DS yang dimiliki zona yang di-hosting untuk zona anak yang merupakan bagian dari rantai kepercayaan.
2. Hapus catatan DS dari zona induk. Lewati langkah ini jika Anda memiliki pulau kepercayaan (tidak ada catatan DS di zona induk dan tidak ada catatan DS untuk zona anak di zona ini).
3. Jika Anda tidak dapat menghapus catatan DS, untuk menghapus zona dari rantai kepercayaan, hapus catatan NS dari zona induk. Untuk informasi selengkapnya, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

Langkah-langkah tambahan berikut memungkinkan Anda memantau efektivitas langkah-langkah individual untuk menghindari masalah ketersediaan DNS di zona Anda.

Cara menonaktifkan penandatanganan DNSSEC

1. Pantau ketersediaan zona.

Anda dapat memantau zona untuk ketersediaan nama domain Anda. Ini dapat membantu Anda mengatasi masalah apa pun yang mungkin memerlukan mundur selangkah setelah Anda mengaktifkan penandatanganan DNSSEC. Anda dapat memantau nama domain Anda dengan sebagian besar lalu lintas dengan menggunakan pencatatan kueri. Untuk informasi selengkapnya tentang menyiapkan pencatatan kueri, lihat [Memantau Amazon Route 53](#).

Pemantauan dapat dilakukan melalui skrip shell, atau melalui layanan berbayar. Namun, seharusnya tidak menjadi satu-satunya sinyal untuk menentukan apakah rollback diperlukan. Anda mungkin juga mendapatkan umpan balik dari pelanggan Anda karena domain tidak tersedia.

2. Temukan DS TTL saat ini.

Anda dapat menemukan DS TTL dengan menjalankan perintah Unix berikut:

```
dig -t DS example.com example.com
```

3. Temukan NS TTL maksimum.

Ada 2 set catatan NS yang terkait dengan zona Anda:

- Catatan NS delegasi — ini adalah catatan NS untuk zona Anda yang dipegang oleh zona induk. Anda dapat menemukan ini dengan menjalankan perintah Unix berikut:

Pertama temukan NS zona induk Anda (jika zona Anda adalah example.com, zona induknya adalah com):

```
dig -t NS com
```

Pilih salah satu catatan NS dan kemudian jalankan yang berikut ini:

```
dig @one of the NS records of your parent zone -t NS example.com
```

Contoh:

```
dig @b.gtld-servers.net. -t NS example.com
```

- Catatan NS dalam zona — ini adalah catatan NS di zona Anda. Anda dapat menemukan ini dengan menjalankan perintah Unix berikut:

```
dig @one of the NS records of your zone -t NS example.com
```

Contoh:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

Perhatikan TTL maksimum untuk kedua zona.

4. Hapus catatan DS dari zona induk.

Hubungi pemilik zona induk untuk menghapus catatan DS.

Rollback: masukkan kembali catatan DS, konfirmasi penyisipan DS efektif, dan tunggu TTL NS (bukan DS) maksimum sebelum semua resolver mulai memvalidasi lagi.

5. Konfirmasikan penghapusan DS efektif.

Jika zona induk ada di layanan DNS Route 53, pemilik zona induk dapat mengonfirmasi propagasi penuh melalui API. [GetChange](#)

Jika tidak, Anda dapat secara berkala menyelidiki zona induk untuk catatan DS, dan kemudian menunggu 10 menit setelahnya untuk meningkatkan kemungkinan penghapusan catatan DS disebarkan sepenuhnya. Perhatikan bahwa beberapa pendaftar telah menjadwalkan penghapusan DS, misalnya sekali sehari.

6. Tunggu DS TTL.

Tunggu sampai semua resolver telah kedaluwarsa catatan DS dari cache mereka.

7. Nonaktifkan penandatanganan DNSSEC dan nonaktifkan kunci penandatanganan kunci (KSK).

- [CLI](#)
- [Konsol](#)

CLI

Hubungi [DisableHostedZoneDNSSEC](#) dan [DeactivateKeySigningKey](#) APIs

Contoh:

```
aws --region us-east-1 route53 disable-hosted-zone-dnssec \
    --hosted-zone-id $hostedzone_id

aws --region us-east-1 route53 deactivate-key-signing-key \
    --hosted-zone-id $hostedzone_id --name $ksk_name
```

Console

Untuk menonaktifkan penandatanganan DNSSEC

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang di-hosting, lalu pilih zona yang di-hosting dengan penandatanganan DNSSEC yang ingin Anda nonaktifkan.
3. Di tab Penandatanganan DNSSEC, pilih Nonaktifkan penandatanganan DNSSEC.
4. Di halaman Nonaktifkan penandatanganan, pilih salah satu opsi berikut, tergantung skenario Anda untuk zona dengan penandatanganan DNSSEC yang dinonaktifkan.
 - Zona induk saja — Zona ini memiliki zona induk dengan catatan DS. Dalam skenario ini, Anda harus menghapus catatan DS zona induk.
 - Zona anak saja — Zona ini memiliki catatan DS untuk rantai kepercayaan dengan satu atau lebih zona anak. Dalam skenario ini, Anda harus menghapus catatan DS zona.

- Zona induk dan anak — Zona ini memiliki catatan DS untuk rantai kepercayaan dengan satu atau lebih zona anak dan zona induk dengan catatan DS. Dalam skenario ini, lakukan hal-hal berikut, untuk dapat:
 - a. Menghapus catatan DS zona.
 - b. Menghapus catatan DS zona induk.

Jika Anda memiliki pulau kepercayaan, Anda dapat melewati langkah ini.

5. Tentukan apa TTL untuk setiap catatan DS yang Anda hapus di Langkah 4. , Pastikan periode TTL terpanjang telah kedaluwarsa.
6. Pilih kotak centang untuk mengonfirmasi bahwa Anda telah mengikuti langkah-langkah secara berurutan.
7. Ketik Nonaktifkan di bidang, seperti yang ditampilkan, lalu pilih Nonaktifkan.

Untuk menonaktifkan kunci penandatanganan kunci (KSK)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang dihosting, lalu pilih zona yang dihosting yang ingin Anda nonaktifkan kunci penandatanganan kunci (KSK).
3. Di bagian Tombol penandatanganan kunci (KSKs), pilih KSK yang ingin Anda nonaktifkan, dan di bawah Tindakan, pilih Edit KSK, atur status KSK ke Tidak Aktif, lalu pilih Simpan KSK.

Rollback: [panggilan ActivateKeySigningKey dan EnableHostedZone DNSSEC](#). APIs

Contoh:

```
aws --region us-east-1 route53 activate-key-signing-key \
    --hosted-zone-id $hostedzone_id --name $ksk_name

aws --region us-east-1 route53 enable-hosted-zone-dnssec \
    --hosted-zone-id $hostedzone_id
```

8. Konfirmasikan penonaktifan penandatanganan zona efektif.

Gunakan Id dari `EnableHostedZoneDNSSEC()` panggilan untuk menjalankan [GetChange](#) untuk memastikan bahwa semua Server DNS Route 53 telah berhenti menandatangani tanggapan (status =INSYNC).

9. Amati resolusi nama.

Anda harus mengamati bahwa tidak ada masalah yang mengakibatkan resolver memvalidasi zona Anda. Biarkan 1-2 minggu untuk memperhitungkan waktu yang dibutuhkan pelanggan Anda untuk melaporkan masalah kepada Anda.

10. (Opsional) Bersihkan.

Jika Anda tidak akan mengaktifkan kembali penandatanganan, Anda dapat membersihkan KSKs [DeleteKeySigningKey](#) dan menghapus kunci yang dikelola pelanggan yang sesuai untuk menghemat biaya.

Bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC

Saat Anda mengaktifkan penandatanganan DNSSEC di Amazon Route 53, Route 53 akan membuat kunci penandatanganan kunci (KSK) untuk Anda. Untuk membuat KSK, Route 53 harus menggunakan kunci yang dikelola pelanggan AWS Key Management Service yang mendukung DNSSEC. Bagian ini menjelaskan detail dan persyaratan untuk kunci yang dikelola pelanggan yang berguna untuk diketahui saat Anda bekerja dengan DNSSEC.

Ingatlah hal-hal berikut saat Anda bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC:

- Kunci terkelola pelanggan yang Anda gunakan dengan penandatanganan DNSSEC harus berada di Wilayah AS Timur (Virginia N.).
- Kunci yang dikelola pelanggan harus berupa kunci yang [dikelola pelanggan asimetris dengan spesifikasi kunci ECC_NIST_P256](#). Kunci yang dikelola pelanggan ini hanya digunakan untuk penandatanganan dan verifikasi. Untuk bantuan membuat kunci terkelola pelanggan asimetris, lihat [Membuat kunci terkelola pelanggan asimetris](#) di Panduan AWS Key Management Service Pengembang. Untuk bantuan menemukan konfigurasi kriptografi dari kunci terkelola pelanggan yang sudah ada, lihat [Melihat konfigurasi kriptografi kunci yang dikelola pelanggan di Panduan AWS Key Management Service Pengembang](#).
- Jika Anda membuat sendiri kunci terkelola pelanggan untuk digunakan dengan DNSSEC di Route 53, Anda harus menyertakan pernyataan kebijakan kunci tertentu yang memberikan izin yang

diperlukan kepada Route 53. Route 53 harus dapat mengakses kunci yang dikelola pelanggan Anda sehingga dapat membuat KSK untuk Anda. Untuk informasi selengkapnya, lihat [Route 53 izin kunci terkelola pelanggan yang diperlukan untuk penandatanganan DNSSEC](#).

- Route 53 dapat membuat kunci terkelola pelanggan untuk Anda gunakan dengan penandatanganan DNSSEC tanpa izin tambahan AWS KMS. Namun, Anda harus memiliki izin khusus jika ingin mengedit kunci setelah dibuat. Izin khusus yang harus Anda miliki adalah sebagai berikut: `kms:UpdateKeyDescription`, `kms:UpdateAlias`, dan `kms:PutKeyPolicy`.
- Ketahuilah bahwa biaya terpisah berlaku untuk setiap kunci terkelola pelanggan yang Anda miliki, apakah Anda membuat kunci yang dikelola pelanggan atau Route 53 membuatnya untuk Anda. Untuk informasi selengkapnya, lihat [harga AWS Key Management Service](#).

Bekerja dengan kunci penandatanganan kunci () KSKs

Jika Anda mengaktifkan penandatanganan DNSSEC, Route 53 membuat kunci penandatanganan kunci (KSK) untuk Anda. Anda dapat memiliki hingga dua KSKs per zona yang dihosting di Route 53. Setelah mengaktifkan penandatanganan DNSSEC, Anda dapat menambahkan, menghapus, atau mengedit KSKs.

Perhatikan hal berikut ketika Anda bekerja dengan KSKs:

- Sebelum dapat menghapus KSK, Anda harus mengedit KSK untuk mengatur statusnya ke Tidak aktif.
- Jika penandatanganan DNSSEC diaktifkan untuk zona yang di-hosting, Route 53 membatasi TTL menjadi satu minggu. Jika Anda menetapkan TTL untuk catatan di zona yang di-hosting ke lebih dari satu minggu, Anda tidak akan mendapatkan kesalahan, namun Route 53 memberlakukan TTL selama satu minggu.
- Untuk membantu mencegah pemadaman zona dan menghindari masalah tidak tersedianya domain Anda, Anda harus cepat mengatasi dan menyelesaikan kesalahan DNSSEC. Kami sangat menyarankan agar Anda mengatur CloudWatch alarm yang memberi tahu Anda setiap kali `DNSSECKeySigningKeysNeedingAction` kesalahan `DNSSECInternalFailure` atau terdeteksi. Untuk informasi selengkapnya, lihat [Memantau zona yang dihosting menggunakan Amazon CloudWatch](#).
- Operasi KSK yang dijelaskan di bagian ini memungkinkan Anda untuk memutar zona Anda. KSKs Untuk informasi selengkapnya dan step-by-step contoh, lihat Rotasi Kunci DNSSEC di posting blog [Mengonfigurasi penandatanganan dan validasi DNSSEC](#) dengan Amazon Route 53.

Untuk bekerja dengan KSKs di Konsol Manajemen AWS, ikuti panduan di bagian berikut.

Menambahkan kunci penandatanganan kunci (KSK)

Jika Anda mengaktifkan penandatanganan DNSSEC, Route 53 membuat kunci penandatanganan kunci (KSK) untuk Anda. Anda juga dapat menambahkan KSKs secara terpisah. Anda dapat memiliki hingga dua KSKs per zona yang dihosting di Route 53.

Ketika Anda membuat KSK, Anda harus menyediakan atau meminta Route 53 untuk membuat kunci yang dikelola pelanggan untuk digunakan dengan KSK. Saat Anda memberikan atau membuat kunci yang dikelola pelanggan, ada beberapa persyaratan. Untuk informasi selengkapnya, lihat [Bekerja dengan kunci yang dikelola pelanggan untuk DNSSEC](#).

Ikuti langkah-langkah berikut untuk menambahkan KSK di Konsol Manajemen AWS.

Cara menambahkan KSK

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang di-hosting, lalu pilih zona yang di-hosting.
3. Pada tab penandatanganan DNSSEC, di bawah Tombol penandatanganan kunci (KSKs), pilih Beralih ke tampilan lanjutan, lalu, di bawah Tindakan, pilih Tambahkan KSK.
4. Di bawah KSK, masukkan nama untuk KSK yang akan dibuat Route 53 untuk Anda. Nama dapat mencakup angka, huruf, dan garis bawah (_). Nama ini harus unik.
5. Masukkan alias untuk kunci terkelola pelanggan yang berlaku untuk penandatanganan DNSSEC, atau masukkan alias untuk kunci terkelola pelanggan baru yang akan dibuat Route 53 untuk Anda.

Note

Jika Anda memilih agar Route 53 membuat kunci terkelola pelanggan, ketahuilah bahwa biaya terpisah berlaku untuk setiap kunci yang dikelola pelanggan. Untuk informasi selengkapnya, lihat [harga AWS Key Management Service](#).

6. Pilih Buat KSK.

Mengedit kunci penandatanganan kunci (KSK)

Anda dapat mengedit status KSK agar menjadi Aktif atau Tidak aktif. Ketika KSK aktif, Route 53 menggunakan KSK untuk penandatanganan DNSSEC. Sebelum dapat menghapus KSK, Anda harus mengedit KSK untuk mengatur statusnya ke Tidak aktif.

Ikuti langkah-langkah berikut untuk mengedit KSK di Konsol Manajemen AWS.

Cara mengedit KSK

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang di-hosting, lalu pilih zona yang di-hosting.
3. Pada tab penandatanganan DNSSEC, di bawah Tombol penandatanganan kunci (KSKs), pilih Beralih ke tampilan lanjutan, lalu, di bawah Tindakan, pilih Edit KSK.
4. Lakukan pembaruan yang diinginkan ke KSK, lalu pilih Simpan.

Menghapus kunci penandatanganan kunci (KSK)

Sebelum dapat menghapus KSK, Anda harus mengedit KSK untuk mengatur statusnya ke Tidak aktif.

Salah satu alasan Anda menghapus KSK adalah sebagai bagian dari rotasi kunci rutin. Memutar kunci kriptografi secara berkala merupakan praktik terbaik. Organisasi mungkin memiliki panduan standar terkait seberapa sering Anda harus merotasi kunci.

Ikuti langkah-langkah berikut untuk menghapus KSK di Konsol Manajemen AWS.

Cara menghapus KSK

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Zona yang di-hosting, lalu pilih zona yang di-hosting.
3. Pada tab penandatanganan DNSSEC, di bawah Tombol penandatanganan kunci (KSKs), pilih Beralih ke tampilan lanjutan, lalu di bawah Tindakan, pilih Hapus KSK.
4. Ikuti panduan untuk mengonfirmasi penghapusan KSK.

Kunci KMS dan manajemen ZSK di Route 53

Bagian ini menjelaskan praktik saat ini yang digunakan Route 53 untuk zona aktif penandatanganan DNSSEC Anda.

Note

Route 53 menggunakan aturan berikut yang mungkin berubah. Setiap perubahan di masa depan tidak akan mengurangi postur keamanan zona atau Route 53 Anda.

Bagaimana Route 53 menggunakan yang AWS KMS terkait dengan KSK Anda

Dalam DNSSEC, KSK digunakan untuk menghasilkan tanda tangan catatan sumber daya (RRSIG) untuk kumpulan catatan sumber daya DNSKEY. Semua ACTIVE KSKs digunakan dalam generasi RRSIG. Route 53 menghasilkan RRSIG dengan memanggil Sign AWS KMS API pada kunci KMS terkait. Untuk informasi selengkapnya, lihat [Masuk](#) panduan AWS KMS API. Ini RRSIGs tidak dihitung terhadap batas set catatan sumber daya zona.

RRSIG memiliki kedaluwarsa. Untuk RRSIGs mencegah kedaluwarsa, disegarkan RRSIGs secara teratur dengan meregenerasinya setiap satu hingga tujuh hari.

RRSIGs Ini juga disegarkan setiap kali Anda memanggil salah satu dari ini APIs:

- [ActivateKeySigningKey](#)
- [CreateKeySigningKey](#)
- [DeactivateKeySigningKey](#)
- [DeleteKeySigningKey](#)
- [DisableHostedZoneDNSSEC](#)
- [EnableHostedZoneDNSSEC](#)

Setiap kali Route 53 melakukan penyegaran, kami menghasilkan 15 RRSIGs untuk mencakup beberapa hari ke depan jika kunci KMS terkait menjadi tidak dapat diakses. Untuk estimasi biaya utama KMS, Anda dapat mengasumsikan penyegaran reguler sekali sehari. Kunci KMS mungkin menjadi tidak dapat diakses oleh perubahan yang tidak disengaja pada kebijakan kunci KMS. Kunci KMS yang tidak dapat diakses akan menyetel status KSK terkait ke. ACTION_NEEDED Kami sangat menyarankan Anda memantau kondisi ini dengan mengatur CloudWatch alarm setiap kali

DNSSECKeySigningKeysNeedingAction kesalahan terdeteksi karena memvalidasi resolver akan mulai gagal pencarian setelah RRSIG terakhir kedaluwarsa. Untuk informasi selengkapnya, lihat [Memantau zona yang dihosting menggunakan Amazon CloudWatch](#).

Bagaimana Route 53 mengelola ZSK zona Anda

Setiap zona host baru dengan penandatanganan DNSSEC diaktifkan akan memiliki satu kunci penandatanganan ACTIVE zona (ZSK). ZSK dibuat secara terpisah untuk setiap zona yang dihosting dan dimiliki oleh Route 53. Algoritma kunci saat ini adalah ECDSAP256SHA256.

Kami akan mulai melakukan rotasi ZSK reguler di zona dalam waktu 7-30 hari sejak dimulainya penandatanganan. Saat ini, Route 53 menggunakan metode Pre-Publish Key Rollover. Untuk informasi selengkapnya, lihat [Rollover Kunci Penandatanganan Zona Pra-Publikasikan](#). Metode ini akan memperkenalkan ZSK lain ke zona tersebut. Rotasi akan diulang setiap 7-30 hari.

Route 53 akan menangguhkan rotasi ZSK jika salah satu zona KSK berada dalam ACTION_NEEDED status karena Route 53 tidak akan dapat meregenerasi set catatan sumber daya DNSKEY untuk memperhitungkan perubahan di ZSK zona. RRSIGs Rotasi ZSK akan secara otomatis dilanjutkan setelah kondisi dibersihkan.

Bukti DNSSEC tentang ketidakberadaan di Route 53

Note

Route 53 menggunakan aturan berikut yang mungkin berubah. Setiap perubahan di masa depan tidak akan mengurangi postur keamanan zona atau Route 53 Anda.

Ada tiga jenis bukti ketidakberadaan di DNSSEC:

- Bukti tidak adanya catatan yang cocok dengan nama kueri.
- Bukti tidak adanya tipe yang cocok dengan tipe kueri.
- Bukti keberadaan catatan wildcard yang digunakan untuk menghasilkan catatan sebagai tanggapan.

Route 53 mengimplementasikan bukti tidak adanya catatan yang cocok dengan nama kueri menggunakan metode BL. Untuk informasi lebih lanjut, lihat [BL](#). Ini adalah metode yang menghasilkan representasi kompak dari bukti dan mencegah zona berjalan.

Dalam kasus di mana ada catatan yang cocok dengan nama kueri tetapi bukan jenis kueri (seperti kueri untuk `web.example.com/AAAA` but there is only `web.example.com/Apresent`), kami mengembalikan catatan NSEC (next secure) minimal yang berisi semua jenis catatan sumber daya yang didukung.

Ketika Route 53 mensintesis jawaban dari catatan wildcard, respons tidak akan disertai dengan catatan aman berikutnya, atau catatan NSEC untuk wildcard. Catatan NSEC semacam itu digunakan dalam beberapa implementasi, biasanya yang melakukan penandatanganan offline, untuk mencegah tanda tangan catatan sumber daya (RRSIG) dalam respons digunakan kembali untuk menipu respons yang berbeda. Route 53 menggunakan penandatanganan online untuk catatan non-DNSkey untuk menghasilkan RRSIGs spesifik untuk respons yang tidak dapat digunakan kembali untuk respons yang berbeda.

Memecahkan masalah penandatanganan DNSSEC

Informasi di bagian ini dapat membantu Anda mengatasi masalah dengan penandatanganan DNSSEC, termasuk mengaktifkan, menonaktifkan, dan dengan kunci penandatanganan kunci (). KSKs

Mengaktifkan DNSSEC

Pastikan Anda telah membaca prasyarat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#) sebelum Anda mulai mengaktifkan penandatanganan DNSSEC.

Menonaktifkan DNSSEC

Untuk menonaktifkan DNSSEC dengan aman, Route 53 akan memeriksa apakah zona target berada dalam rantai kepercayaan. Ini memeriksa apakah induk dari zona target memiliki catatan NS dari zona target dan catatan DS dari zona target. Jika zona target tidak dapat diselesaikan secara publik, misalnya, mendapatkan respons SERVFAIL saat menanyakan NS dan DS, Route 53 tidak dapat menentukan apakah aman untuk menonaktifkan DNSSEC. Anda dapat menghubungi zona induk Anda untuk memperbaiki masalah tersebut, dan coba lagi menonaktifkan DNSSEC nanti.

Status KSK adalah Diperlukan tindakan

KSK dapat mengubah statusnya menjadi Tindakan yang diperlukan (atau ACTION_NEEDED dalam [KeySigningKey](#) status), ketika Route 53 DNSSEC kehilangan akses ke yang sesuai AWS KMS key (karena perubahan izin atau penghapusan). AWS KMS key

Jika status KSK diperlukan Tindakan, itu berarti bahwa pada akhirnya itu akan menyebabkan pemadaman zona untuk klien yang menggunakan DNSSEC memvalidasi resolver dan Anda harus bertindak cepat untuk mencegah zona produksi menjadi tidak dapat diselesaikan.

Untuk memperbaiki masalah, pastikan bahwa kunci terkelola pelanggan yang menjadi dasar KSK Anda diaktifkan dan memiliki izin yang benar. Untuk informasi lebih lanjut tentang izin yang diperlukan, lihat [Route 53 izin kunci terkelola pelanggan yang diperlukan untuk penandatanganan DNSSEC](#).

Setelah Anda memperbaiki KSK, aktifkan lagi dengan menggunakan konsol atau AWS CLI, seperti yang dijelaskan dalam [Langkah 2: Aktifkan penandatanganan DNSSEC dan buat KSK](#).

Untuk mencegah masalah ini di masa mendatang, pertimbangkan untuk menambahkan Amazon CloudWatch metrik untuk melacak keadaan KSK seperti yang disarankan di [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

Status KSK adalah Kegagalan internal

Ketika KSK memiliki status kegagalan internal (atau `INTERNAL_FAILURE` dalam [KeySigningKey](#) status), Anda tidak dapat bekerja dengan entitas DNSSEC lainnya sampai masalah teratasi. Anda harus mengambil tindakan sebelum dapat bekerja dengan penandatanganan DNSSEC, termasuk bekerja dengan KSK ini atau KSK lainnya.

Untuk memperbaiki masalah, coba aktifkan lagi atau nonaktifkan KSK.

[Untuk memperbaiki masalah saat bekerja dengan APIs, coba aktifkan penandatanganan \(EnableHostedZoneDNSSEC\) atau nonaktifkan penandatanganan \(DNSSEC\). DisableHostedZone](#)

Anda harus segera memperbaiki masalah Kegagalan internal. Anda tidak dapat membuat perubahan lain ke zona yang di-hosting hingga masalah diperbaiki, kecuali operasi untuk memperbaiki Kegagalan internal.

Menggunakan AWS Cloud Map untuk membuat catatan dan pemeriksaan kesehatan

Jika ingin merutekan lalu lintas internet atau lalu lintas dalam Amazon VPC ke komponen aplikasi atau layanan mikro, Anda dapat menggunakan AWS Cloud Map untuk membuat catatan secara otomatis dan, secara opsional, untuk membuat pemeriksaan kondisi. Lihat informasi selengkapnya di [Panduan Developer AWS Cloud Map](#).

Kendala dan perilaku DNS

Olahpesan DNS tunduk pada faktor-faktor yang memengaruhi cara Anda membuat dan menggunakan zona serta catatan yang di-hosting. Bagian ini menjelaskan faktor-faktor tersebut.

Ukuran respons maksimum

Untuk memenuhi standar DNS, ukuran respons yang dikirim melalui UDP tidak lebih dari 512 byte. Respons yang melebihi 512 byte akan dipotong dan penyelesai harus mengeluarkan kembali permintaan melalui TCP. Jika resolver mendukung EDNS0 (seperti yang didefinisikan dalam [RFC 2671](#)), dan mengiklankan opsi EDNS0 ke Amazon Route 53, Route 53 mengizinkan respons hingga 4096 byte melalui UDP, tanpa pemotongan.

Pemrosesan bagian otoritatif

Agar kueri berhasil, Route 53 menambahkan catatan nama server (NS) untuk zona yang di-hosting yang relevan ke bagian Otoritas respons DNS. Untuk nama yang tidak ditemukan (respons NXDOMAIN), Route 53 menambahkan catatan Start of Authority (SOA) (seperti yang ditentukan dalam [RFC 1035](#)) untuk zona yang di-hosting yang relevan ke bagian Otoritas respons DNS.

Pemrosesan bagian tambahan

Route 53 menambahkan catatan ke bagian Tambahan. Jika catatan diketahui dan sesuai, layanan menambahkan catatan A atau AAAA untuk setiap target catatan MX, CNAME, NS, atau SRV yang dikutip di bagian Jawaban. Untuk informasi selengkapnya tentang tipe catatan DNS ini, lihat [Tipe data DNS yang didukung](#).

Topik terkait

Untuk informasi tentang mentransfer pendaftaran domain (bukan hanya hosting DNS) ke Route 53, lihat topik berikut:

- [Daftar periksa pra-transfer untuk transfer domain](#)— Lengkapi daftar periksa ini sebelum mentransfer pendaftaran domain untuk menghindari kegagalan transfer umum.
- [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#)— Step-by-step proses untuk mentransfer pendaftaran domain dari registrar lain ke Route 53.
- [Mentransfer domain](#)— Ikhtisar semua opsi transfer domain, termasuk transfer antar AWS akun.

Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS

Arus Lalu Lintas sangat menyederhanakan proses pembuatan dan pemeliharaan catatan dalam konfigurasi besar dan kompleks.

Mengelola catatan terkait di zona yang di-hosting dapat menjadi tantangan dalam situasi berikut:

- Anda memiliki banyak sumber daya yang melakukan operasi yang sama, seperti server web yang melayani lalu lintas untuk domain yang sama.
- Anda ingin membuat sebuah pohon kompleks catatan menggunakan [catatan alias](#) dan kombinasi dari [Kebijakan perutean Route 53](#), seperti latensi, failover, dan tertimbang.

Keuntungan Arus Lalu Lintas

Untuk mempermudah melacak catatan dan hubungannya, Traffic Flow menyederhanakan pembuatan catatan DNS dengan fitur-fitur berikut:

Editor visual

Editor visual Traffic Flow memungkinkan Anda membuat pohon catatan yang kompleks dan melihat hubungan di antara catatan. Misalnya, Anda dapat membuat konfigurasi di mana alias latensi mencatat catatan tertimbang referensi, dan catatan tertimbang mereferensikan sumber daya Anda dalam beberapa wilayah AWS. Setiap konfigurasi dikenal sebagai kebijakan lalu lintas. Anda dapat membuat kebijakan lalu lintas sebanyak yang Anda inginkan tanpa biaya.

Penentuan versi

Anda dapat membuat beberapa versi kebijakan lalu lintas sehingga Anda tidak perlu memulai dari awal ketika konfigurasi berubah. Versi lama terus ada hingga Anda menghapusnya; ada batas default 1000 versi per kebijakan lalu lintas. Anda dapat secara opsional memberikan setiap versi deskripsi.

Pembuatan dan pembaruan catatan otomatis

Kebijakan lalu lintas dapat mewakili puluhan atau bahkan ratusan catatan. Arus Lalu Lintas memungkinkan Anda membuat semua catatan tersebut secara otomatis dengan membuat catatan kebijakan lalu lintas. Anda menentukan zona yang di-hosting dan nama catatan pada dasar

struktur, seperti `example.com` atau `www.example.com`, dan Route 53 secara otomatis membuat semua catatan lain di struktur tersebut. Catatan dasar, catatan kebijakan lalu lintas—muncul dalam daftar rekaman untuk zona yang di-hosting; semua catatan lainnya disembunyikan.

Ketika Anda membuat versi baru dari kebijakan lalu lintas, Anda dapat secara selektif memperbarui catatan kebijakan lalu lintas yang Anda buat menggunakan versi kebijakan lalu lintas sebelumnya. Ketika Anda memperbarui catatan kebijakan lalu lintas, Route 53 secara otomatis memperbarui semua catatan lain pada struktur. Anda juga dapat dengan cepat memutar kembali perubahan dengan memperbarui catatan kebijakan lalu lintas lagi untuk menggunakan versi sebelumnya dari kebijakan lalu lintas.

 Note

Anda dapat menggunakan Arus Lalu Lintas untuk membuat catatan hanya di zona yang dihosting publik.

Kebijakan perutean geoproximity

Saat menggunakan Arus Lalu Lintas, Anda dapat lebih intuitif memahami bagaimana lalu lintas diarahkan ke setiap titik akhir global Anda dengan menggunakan peta geoproximity pada editor visual Arus Lalu Lintas. Untuk informasi selengkapnya, lihat [Perutean geoproksimitas](#).

Gunakan kembali untuk beberapa catatan di zona yang di-hosting lainnya

Anda dapat menggunakan kebijakan lalu lintas untuk secara otomatis membuat catatan di beberapa zona yang di-hosting publik. Misalnya, jika Anda menggunakan server web yang sama untuk beberapa nama domain, Anda dapat menggunakan kebijakan lalu lintas yang sama untuk membuat catatan kebijakan lalu lintas di zona yang di-hosting untuk `example.com`, `example.org`, dan `example.net`.

Ketika klien mengajukan permintaan untuk nama catatan akar, seperti `example.com` atau `www.example.com`, Route 53 menanggapi permintaan berdasarkan konfigurasi dalam kebijakan lalu lintas yang Anda gunakan untuk membuat catatan kebijakan lalu lintas yang sesuai.

Ada biaya bulanan untuk setiap catatan kebijakan lalu lintas. Untuk informasi selengkapnya, lihat bagian "Arus lalu lintas" [Amazon Route 53](#).

Untuk meminimalkan biaya ini, Anda dapat membuat satu atau lebih alias catatan di zona yang di-hosting yang mereferensikan catatan kebijakan lalu lintas di zona yang di-hosting. Misalnya, Anda

dapat membuat catatan kebijakan lalu lintas untuk example.com dan kemudian membuat catatan alias untuk www.example.com yang merujuk catatan kebijakan lalu lintas.

Membuat dan mengelola kebijakan lalu lintas

Topik

- [Membuat kebijakan lalu lintas](#)
- [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#)
- [Melihat peta yang menunjukkan efek pengaturan geoproximity](#)
- [Membuat versi tambahan dari kebijakan lalu lintas](#)
- [Membuat kebijakan lalu lintas dengan menggunakan dokumen JSON](#)
- [Melihat versi kebijakan lalu lintas dan catatan kebijakan terkait](#)
- [Menghapus versi kebijakan lalu lintas dan kebijakan lalu lintas](#)

Membuat kebijakan lalu lintas

Untuk membuat kebijakan lalu lintas, lakukan prosedur berikut.

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk membuat kebijakan lalu lintas

1. Desain konfigurasi Anda. Untuk informasi tentang cara kerja konfigurasi perutean DNS kompleks, lihat [Mengonfigurasi failover DNS](#) di [Membuat pemeriksaan kesehatan Amazon Route 53](#).
2. Berdasarkan desain untuk konfigurasi Anda, buat pemeriksaan kondisi yang ingin Anda gunakan untuk titik akhir Anda.
3. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
4. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
5. Pilih Create traffic policy (Buat kebijakan lalu lintas).
6. Masukkan nama dan deskripsi opsional, lalu pilih Berikutnya.
7. Pada editor, pilih jenis catatan sumber daya DNS di panel Properties. Jenis ini akan ditetapkan ke semua catatan sumber daya yang Anda buat untuk kebijakan lalu lintas ini.

Pilih Konfirmasi. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).

8. Di halaman editor, pilih Connect to dan kemudian pilih salah satu Aturan perutean baru, Titik akhir baru, Aturan perutean yang ada, atau Titik akhir yang ada. Jika Anda memilih aturan perutean baru, di panel Properti pilih aturan perutean dan pilih Konfirmasi. Kemudian, di panel Properties, masukkan nilai yang sesuai. Ulangi proses ini sampai kebijakan Anda selesai. Untuk informasi selengkapnya tentang nilai untuk setiap jenis koneksi, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).

Anda dapat menghapus aturan, titik akhir, dan cabang kebijakan lalu lintas dengan cara berikut:

- Untuk menghapus aturan atau titik akhir, pilih aturan atau titik akhir di editor, lalu pilih Hapus di panel Properti.

Important

Jika Anda menghapus aturan yang memiliki aturan turunan dan titik akhir, Amazon Route 53 juga menghapus semua turunannya.

- Jika Anda menghubungkan dua aturan ke aturan anak atau titik akhir yang sama dan Anda ingin menghapus salah satu koneksi, pilih koneksi yang ingin Anda hapus, dan pilih Hapus di panel Properti untuk koneksi tersebut.

9. Pilih Buat kebijakan.
10. Pada halaman Buat catatan kebijakan, gunakan kebijakan lalu lintas baru untuk membuat satu atau beberapa catatan kebijakan di satu zona yang dihosting. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#). Anda juga dapat membuat catatan kebijakan nanti, baik di zona yang di-hosting yang sama atau di zona yang di-hosting tambahan.

Jika Anda tidak ingin membuat catatan kebijakan sekarang, pilih Batal, dan konsol akan menampilkan daftar kebijakan lalu lintas dan catatan kebijakan yang telah Anda buat menggunakan AWS akun saat ini.

11. Jika Anda menetapkan setelan untuk catatan kebijakan pada langkah sebelumnya, pilih Buat catatan kebijakan.

Old console

Untuk membuat kebijakan lalu lintas

1. Desain konfigurasi Anda. Untuk informasi tentang cara kerja konfigurasi perutean DNS kompleks, lihat [Mengonfigurasi failover DNS](#) di [Membuat pemeriksaan kesehatan Amazon Route 53](#).
2. Berdasarkan desain untuk konfigurasi Anda, buat pemeriksaan kondisi yang ingin Anda gunakan untuk titik akhir Anda.
3. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
4. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
5. Pilih Create traffic policy (Buat kebijakan lalu lintas).
6. Pada halaman Kebijakan nama, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).
7. Pilih Next (Berikutnya).
8. Pada halaman Buat kebijakan lalu lintas Nama kebijakan v1, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).

Anda dapat menghapus aturan, titik akhir, dan cabang kebijakan lalu lintas dengan cara berikut:

- Untuk menghapus aturan atau titik akhir, klik x di sudut kanan atas kotak.

 Important

Jika Anda menghapus aturan yang memiliki aturan turunan dan titik akhir, Amazon Route 53 juga menghapus semua turunannya.

- Jika Anda menghubungkan dua aturan untuk aturan turunan yang sama atau titik akhir dan Anda ingin menghapus salah satu sambungan, jeda kursor Anda pada sambungan yang ingin Anda hapus, lalu klik x untuk koneksi itu.
9. Pilih Create traffic policy (Buat kebijakan lalu lintas).
 10. Opsional: Pada Membuat catatan kebijakan dengan kebijakan lalu lintas, gunakan kebijakan lalu lintas baru untuk membuat satu atau lebih catatan kebijakan di satu zona yang di-hosting. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#). Anda juga dapat membuat catatan kebijakan nanti, baik di zona yang di-hosting yang sama atau di zona yang di-hosting tambahan.

Jika Anda tidak ingin membuat catatan kebijakan sekarang, pilih Lewati langkah ini, dan konsol akan menampilkan daftar kebijakan lalu lintas dan catatan kebijakan yang telah Anda buat menggunakan AWS akun saat ini.

11. Jika Anda menetapkan pengaturan untuk catatan kebijakan di langkah sebelumnya, pilih Create policy record (Buat catatan kebijakan).

Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas

 Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama. Daftar berikut berlaku untuk kedua konsol, kecuali jika dicatat.

Ketika Anda membuat kebijakan lalu lintas, Anda menentukan nilai berikut.

-
-
-
-
-
-
-
-

Nama kebijakan

Masukkan nama yang menggambarkan kebijakan lalu lintas. Nilai ini muncul dalam daftar kebijakan lalu lintas di konsol. Anda tidak dapat mengubah nama kebijakan lalu lintas setelah Anda membuatnya.

Versi

Nilai ini ditetapkan secara otomatis oleh Amazon Route 53 ketika Anda membuat kebijakan lalu lintas atau versi baru dari kebijakan yang ada.

Deskripsi versi

Masukkan deskripsi yang berlaku untuk versi kebijakan lalu lintas ini. Nilai ini muncul dalam daftar lalu lintas kebijakan versi di konsol.

Tipe DNS

Pilih jenis DNS yang Anda inginkan Amazon Route 53 untuk menetapkan semua catatan ketika Anda membuat catatan kebijakan dengan menggunakan versi kebijakan lalu lintas ini. Untuk mengetahui daftar jenis yang didukung, lihat [Tipe data DNS yang didukung](#).

Important

Jika Anda membuat versi baru dari kebijakan lalu lintas yang ada, Anda dapat mengubah jenis DNS. Namun, Anda tidak dapat mengedit catatan kebijakan dan memilih versi kebijakan lalu lintas yang memiliki jenis DNS yang berbeda dari versi kebijakan lalu lintas yang

digunakan untuk membuat catatan kebijakan. Sebagai contoh, jika Anda membuat catatan kebijakan dengan menggunakan versi kebijakan lalu lintas yang memiliki Jenis DNS A, Anda tidak dapat mengedit catatan kebijakan dan memilih versi kebijakan lalu lintas yang memiliki nilai lain untuk Jenis DNS.

Jika Anda ingin merutekan lalu lintas ke AWS sumber daya berikut, pilih nilai yang berlaku:

- CloudFront distribusi - Pilih A: Alamat IP dalam IPv4 format atau AAAA: alamat IP dalam IPv6 format.

 Note

CloudFront alias endpoint tidak mendukung evaluasi pemeriksaan kesehatan. Namun, Anda dapat membuat pemeriksaan kesehatan untuk memantau CloudFront titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

- ELB Application load balancer - Pilih alamat A: IP dalam IPv4 format atau AAAA: alamat IP dalam format. IPv6
- ELB Classic load balancer - Pilih alamat A: IP dalam IPv4 format atau AAAA: alamat IP dalam format. IPv6
- ELB Network load balancer - Pilih alamat A: IP dalam IPv4 format atau AAAA: alamat IP dalam format. IPv6
- Lingkungan Elastic Beanstalk: Pilih A: Alamat IP dalam format. IPv4
- Bucket Amazon S3 dikonfigurasi sebagai titik akhir situs web: Pilih alamat IP A: dalam format. IPv4

Sambungkan ke

Pilih aturan yang berlaku atau titik akhir berdasarkan desain untuk konfigurasi Anda.

Aturan failover

Pilih opsi ini bila Anda ingin mengonfigurasi failover aktif-pasif, di mana satu sumber daya mengambil semua lalu lintas ketika tersedia dan sumber daya lainnya mengambil semua lalu lintas ketika sumber daya pertama tidak tersedia.

Untuk informasi selengkapnya, lihat [Failover active-passive](#).

 Note

Opsi Evaluasi kondisi target dicentang secara default dan akan mengevaluasi kondisi titik akhir target yang menjadi tujuan perutean lalu lintas melalui catatan alias. Jika titik akhir Anda tidak menerima lalu lintas DNS melalui catatan alias, hapus centang dari opsi ini dan buat pemeriksaan kondisi jika Anda ingin memantau kondisi titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Aturan geolokasi

Pilih opsi ini bila Anda ingin Amazon Route 53 untuk menanggapi permintaan DNS berdasarkan lokasi pengguna Anda.

Untuk informasi selengkapnya, lihat [Perutean geolokasi](#).

Bila Anda memilih Aturan geolokasi, Anda juga memilih negara atau negara bagian di Amerika Serikat asal permintaan.

 Note

Opsi Evaluasi kondisi target dicentang secara default dan akan mengevaluasi kondisi titik akhir target yang menjadi tujuan perutean lalu lintas melalui catatan alias. Jika titik akhir Anda tidak menerima lalu lintas DNS melalui catatan alias, hapus centang dari opsi ini dan buat pemeriksaan kondisi jika Anda ingin memantau kondisi titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Latensi aturan

Pilih opsi ini jika Anda memiliki sumber daya di beberapa pusat EC2 data Amazon yang menjalankan fungsi yang sama, dan Anda ingin Route 53 merespons kueri DNS dengan sumber daya yang memberikan latensi terbaik.

Saat Anda memilih aturan Latensi, Anda juga memilih aturan. Wilayah AWS

Untuk informasi selengkapnya, lihat [Perutean berbasis latensi](#).

 Note

Opsi Evaluasi kondisi target dicentang secara default dan akan mengevaluasi kondisi titik akhir target yang menjadi tujuan perutean lalu lintas melalui catatan alias. Jika titik akhir Anda tidak menerima lalu lintas DNS melalui catatan alias, hapus centang dari opsi ini dan buat pemeriksaan kondisi jika Anda ingin memantau kondisi titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Aturan geoproximity

Pilih opsi ini jika Anda ingin Route 53 merespons kueri DNS berdasarkan lokasi sumber daya Anda dan, secara opsional, pada bias yang Anda tentukan. Bias memungkinkan Anda mengirim lebih banyak lalu lintas ke sumber daya atau mengalihkan lebih banyak lalu lintas dari sumber daya.

Jika Anda memilih Aturan geoproximity, masukkan nilai berikut:

Lokasi titik akhir

Pilih nilai yang berlaku:

- Kustom (masukkan koordinat) - Jika titik akhir Anda bukan AWS sumber daya, pilih Kustom (masukkan koordinat).
- An Wilayah AWS - Jika titik akhir Anda adalah AWS sumber daya, pilih sumber daya Wilayah AWS yang Anda buat.
- Zona AWS Lokal — Jika titik akhir Anda adalah AWS sumber daya, pilih Zona AWS Lokal tempat Anda membuat sumber daya.

Jika Anda menggunakan AWS Local Zones, Anda harus mengaktifkannya terlebih dahulu. Untuk informasi selengkapnya, lihat [Memulai Local Zones](#) di Panduan Pengguna AWS Local Zones.

Untuk Local Zones yang tersedia, lihat [Lokasi AWS Local Zones](#).

Untuk mempelajari perbedaan antara Wilayah AWS dan Local Zones, lihat [Wilayah dan Zona](#) di Panduan EC2 Pengguna Amazon.

Important

Kebijakan perutean geoproximity tunggal tidak dapat berisi dua atau lebih lokasi yang secara geografis terletak dalam wilayah metropolitan yang sama.

Selain itu, beberapa Wilayah AWS dan Local Zones, seperti US West (Oregon) dan Portland, AS, terletak terlalu dekat satu sama lain untuk digunakan dalam kebijakan perutean geoproximity yang sama. Jika Anda memerlukan perutean lalu lintas ke lebih dari satu lokasi dalam wilayah metropolitan yang sama, alih-alih tentukan kebijakan perutean geoproximity yang menghasilkan aturan perutean tertimbang 50/50 (WRR) untuk dua titik akhir yang berbeda di area tersebut, sehingga mendistribusikan lalu lintas secara merata di antara titik akhir tersebut.

Koordinat

Jika Anda memilih Kustom (masukkan koordinat) untuk Lokasi Titik Akhir, masukkan garis lintang dan bujur dari lokasi sumber daya. Perhatikan hal-hal berikut:

- Garis lintang mewakili lokasi selatan (negatif) atau utara (positif) dari khatulistiwa. Nilai yang valid adalah -90 derajat sampai 90 derajat.
- Bujur mewakili lokasi barat (negatif) atau timur (positif) dari meridian utama. Nilai yang valid adalah -180 derajat sampai 180 derajat.
- Anda bisa mendapatkan garis lintang dan bujur dari beberapa aplikasi pemetaan online. Misalnya, di Google Maps, URL untuk lokasi menentukan garis lintang dan bujur:

<https://www.google.com/maps/@47.6086111,-122.3409953,20z>

- Anda dapat memasukkan hingga dua desimal presisi, misalnya, 47,63. Jika Anda menentukan nilai dengan presisi yang lebih besar, Route 53 memotong nilai untuk dua tempat setelah desimal. Untuk garis lintang dan bujur di khatulistiwa, 0,01 derajat sekitar 0,69 mil.

Bias

Untuk secara opsional mengubah ukuran wilayah geografis dari mana Route 53 rute lalu lintas ke sumber daya, tentukan nilai yang berlaku untuk Bias:

- Untuk memperluas ukuran wilayah geografis dari mana Route 53 mengarahkan lalu lintas ke sumber daya, tentukan bilangan bulat positif dari 1 sampai 99 untuk bias. Route 53 menyusutkan ukuran wilayah yang berdekatan.

- Untuk menyusutkan ukuran wilayah geografis yang lalu lintasnya dirutekan oleh Route 53 ke sumber daya, tentukan bias negatif -1 sampai -99. Route 53 memperluas ukuran wilayah yang berdekatan.

 Important

Efek mengubah nilai Bias relatif, berdasarkan lokasi sumber daya lain, bukan absolut, berdasarkan jarak. Akibatnya, efek dari perubahan sulit diprediksi. Misalnya, tergantung di mana sumber daya Anda berada, mengubah bias dari 10 menjadi 15 dapat berarti perbedaan antara menambah atau mengurangi jumlah lalu lintas yang signifikan dari wilayah metropolitan New York City. Kami menyarankan Anda mengubah bias sedikit demi sedikit dan mengevaluasi hasilnya, lalu membuat perubahan tambahan jika sesuai.

Untuk informasi selengkapnya, lihat [Perutean geoproksimitas](#).

 Note

Opsi Evaluasi kondisi target dicentang secara default dan akan mengevaluasi kondisi titik akhir target yang menjadi tujuan perutean lalu lintas melalui catatan alias. Jika titik akhir Anda tidak menerima lalu lintas DNS melalui catatan alias, hapus centang dari opsi ini dan buat pemeriksaan kondisi jika Anda ingin memantau kondisi titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Aturan jawaban multinilai

Pilih opsi ini bila Anda ingin Route 53 merespons kueri DNS dengan hingga delapan jawaban sehat, dipilih kira-kira secara acak.

Untuk informasi selengkapnya, lihat [Perutean jawaban multinilai](#).

 Note

Opsi Evaluasi kondisi target dicentang secara default dan akan mengevaluasi kondisi titik akhir target yang menjadi tujuan perutean lalu lintas melalui catatan alias. Jika titik akhir Anda tidak menerima lalu lintas DNS melalui catatan alias, hapus centang dari opsi ini dan

buat pemeriksaan kondisi jika Anda ingin memantau kondisi titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Aturan tertimbang

Pilih opsi ini ketika Anda memiliki beberapa sumber daya yang melakukan fungsi yang sama (misalnya, server web yang melayani situs web yang sama) dan Anda ingin Route 53 untuk merutekan lalu lintas ke sumber daya tersebut dalam proporsi yang Anda tentukan (misalnya, 1/3 ke satu server dan 2/3 ke yang lain).

Jika Anda memilih Aturan tertimbang, masukkan bobot yang ingin Anda terapkan pada aturan ini.

Untuk informasi selengkapnya, lihat [Perutean tertimbang](#).

Note

Opsi Evaluasi kondisi target dicentang secara default dan akan mengevaluasi kondisi titik akhir target yang menjadi tujuan perutean lalu lintas melalui catatan alias. Jika titik akhir Anda tidak menerima lalu lintas DNS melalui catatan alias, hapus centang dari opsi ini dan buat pemeriksaan kondisi jika Anda ingin memantau kondisi titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Titik akhir

Pilih opsi ini untuk menentukan sumber daya, seperti CloudFront distribusi atau penyeimbang beban Elastic Load Balancing, tempat Anda ingin merutekan kueri DNS.

Peran yang sudah ada

Pilih opsi ini saat Anda ingin merutekan kueri DNS ke aturan yang ada dalam kebijakan lalu lintas ini. Misalnya, Anda dapat membuat dua atau beberapa aturan geolokasi yang mengarahkan kueri untuk negara yang berbeda ke aturan failover yang sama. Aturan failover kemudian dapat merutekan kueri ke dua penyeimbang beban Elastic Load Balancing.

Pilihan ini tidak tersedia jika kebijakan lalu lintas tidak menyertakan aturan apa pun.

Titik akhir yang sudah ada

Pilih opsi ini jika Anda ingin merutekan permintaan DNS ke titik akhir yang sudah ada. Misalnya, jika Anda memiliki dua aturan failover, Anda mungkin ingin merutekan kueri DNS untuk opsi On failover (sekunder) ke penyeimbang beban Elastic Load Balancing yang sama.

Pilihan ini tidak tersedia jika kebijakan lalu lintas tidak menyertakan titik akhir apa pun.

Tipe nilai

Pilih opsi yang sesuai:

CloudFront distribusi

Pilih opsi ini jika Anda ingin merutekan lalu lintas ke CloudFront distribusi. Opsi ini hanya tersedia jika Anda memilih A: alamat IP dalam IPv4 format untuk tipe DNS atau AAAA: alamat IP dalam IPv6 format untuk tipe DNS.

Note

CloudFront alias endpoint tidak mendukung evaluasi pemeriksaan kesehatan. Namun, Anda dapat membuat pemeriksaan kesehatan untuk memantau CloudFront titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Penyeimbang beban Aplikasi ELB

Pilih opsi ini jika Anda ingin merutekan lalu lintas ke penyeimbang beban Aplikasi Elastic Load Balancing. Opsi ini hanya tersedia jika Anda memilih alamat A: IP dalam IPv4 format atau AAAA: alamat IP dalam IPv6 format untuk tipe DNS.

ELB Classic penyeimbang beban

Pilih opsi ini jika Anda ingin merutekan lalu lintas ke penyeimbang beban Elastic Load Balancing Classic. Opsi ini hanya tersedia jika Anda memilih alamat A: IP dalam IPv4 format atau AAAA: alamat IP dalam IPv6 format untuk tipe DNS.

Penyeimbang beban Jaringan ELB

Pilih opsi ini jika Anda ingin merutekan lalu lintas ke penyeimbang beban Elastic Load Balancing Network. Opsi ini hanya tersedia jika Anda memilih alamat A: IP dalam IPv4 format atau AAAA: alamat IP dalam IPv6 format untuk tipe DNS.

Lingkungan Elastic Beanstalk

Pilih opsi ini jika Anda ingin mengarahkan lalu lintas ke lingkungan Elastic Beanstalk. Opsi ini hanya tersedia jika Anda memilih A: alamat IP dalam IPv4 format untuk jenis DNS.

Titik akhir situs web S3

Pilih opsi ini jika Anda ingin mengarahkan lalu lintas ke bucket Amazon S3 yang dikonfigurasi sebagai titik akhir situs web. Opsi ini hanya tersedia jika Anda memilih A: alamat IP dalam IPv4 format untuk jenis DNS.

Ketik nilai tipe DNS

Pilih opsi ini jika Anda ingin Route 53 untuk menanggapi permintaan DNS menggunakan nilai dalam bidang Nilai. Misalnya, jika Anda memilih A untuk nilai Tipe DNS ketika Anda membuat kebijakan lalu lintas ini, opsi ini di daftar Tipe nilai akan menjadi nilai Tipe A. Ini mengharuskan Anda memasukkan alamat IP dalam IPv4 format di bidang Nilai. Route 53 akan menanggapi permintaan DNS yang diarahkan ke titik akhir ini dengan alamat IP di bidang Nilai.

Nilai

Pilih atau masukkan nilai berdasarkan opsi yang Anda pilih untuk Tipe nilai:

CloudFront distribusi

Pilih CloudFront distribusi dari daftar distribusi yang terkait dengan AWS akun saat ini.

Penyeimbang beban Aplikasi ELB

Pilih penyeimbang beban Aplikasi Elastic Load Balancing dari daftar load balancer yang terkait dengan akun saat ini. AWS

ELB Classic penyeimbang beban

Pilih penyeimbang beban Elastic Load Balancing Classic dari daftar load balancer yang terkait dengan akun saat ini. AWS

Penyeimbang beban Jaringan ELB

Pilih load balancer Elastic Load Balancing Network dari daftar load balancer yang terkait dengan akun saat ini. AWS

Lingkungan Elastic Beanstalk

Pilih lingkungan Elastic Beanstalk dari daftar lingkungan yang terkait dengan akun. Akun AWS

Titik akhir situs web S3

Pilih bucket Amazon S3 dari daftar bucket Amazon S3 yang dikonfigurasi sebagai titik akhir situs web dan yang terkait dengan akun saat ini. AWS

Important

Ketika Anda membuat catatan kebijakan berdasarkan kebijakan lalu lintas ini, bucket yang Anda pilih di sini harus sesuai dengan nama domain (seperti `www.example.com`) yang Anda tentukan untuk [Policy record DNS name](#) dalam catatan kebijakan. Jika Nilai dan Nama DNS catatan kebijakan tidak cocok, Amazon S3 tidak akan menanggapi permintaan DNS untuk nama domain.

Ketik nilai tipe DNS

Masukkan nilai yang sesuai dengan nilai yang Anda tentukan tipe DNS ketika Anda memulai kebijakan lalu lintas ini. Misalnya, jika Anda memilih MX untuk tipe DNS, masukkan dua nilai: prioritas yang ingin Anda tetapkan ke server email dan nama domain server email, seperti `10 sydney.mail.example.com`.

Untuk informasi lebih lanjut tentang jenis DNS yang didukung, lihat [Tipe data DNS yang didukung](#).

Kunci (hanya konsol baru)

Masukkan nama ramah untuk aturan perutean atau titik akhir untuk Key. Nilai ini ditampilkan sebagai nama node di editor.

Melihat peta yang menunjukkan efek pengaturan geoproximity

Aturan geoproximity memungkinkan Anda menentukan lokasi sumber daya Anda, baik di Wilayah AWS, atau Local Zones, dan, menggunakan lintang dan bujur, di non-lokasi.AWS Saat Anda membuat aturan geoproximity, secara default, Route 53 merutekan lalu lintas internet ke sumber daya yang paling dekat dengan pengguna Anda. Anda juga dapat memilih untuk merutekan lebih banyak lalu lintas atau lebih sedikit lalu lintas ke sumber daya dengan menentukan bias, yang memperluas atau mengecilkan wilayah geografis dari mana lalu lintas diarahkan ke sumber daya. Untuk informasi selengkapnya tentang perutean geoproximity, lihat [Perutean geoproksimitas](#).

Note

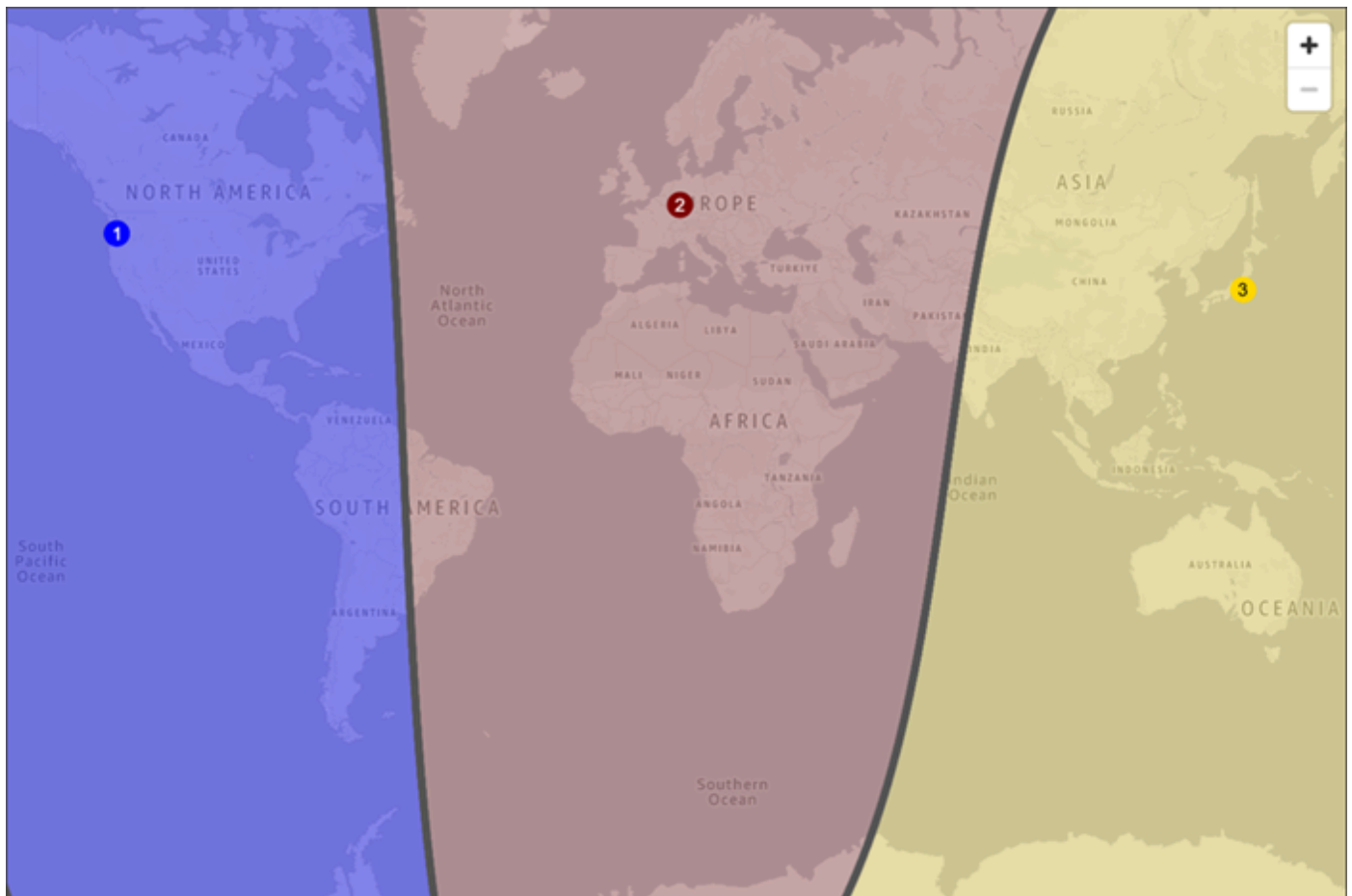
Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Anda dapat menampilkan peta yang menunjukkan efek pengaturan geoproximity Anda saat ini. Misalnya, jika Anda memiliki sumber daya di Wilayah AS Barat (Oregon), Eropa (Frankfurt), dan Asia Pasifik (Tokyo), dan jika Anda tidak menentukan bias, peta akan terlihat seperti ini.



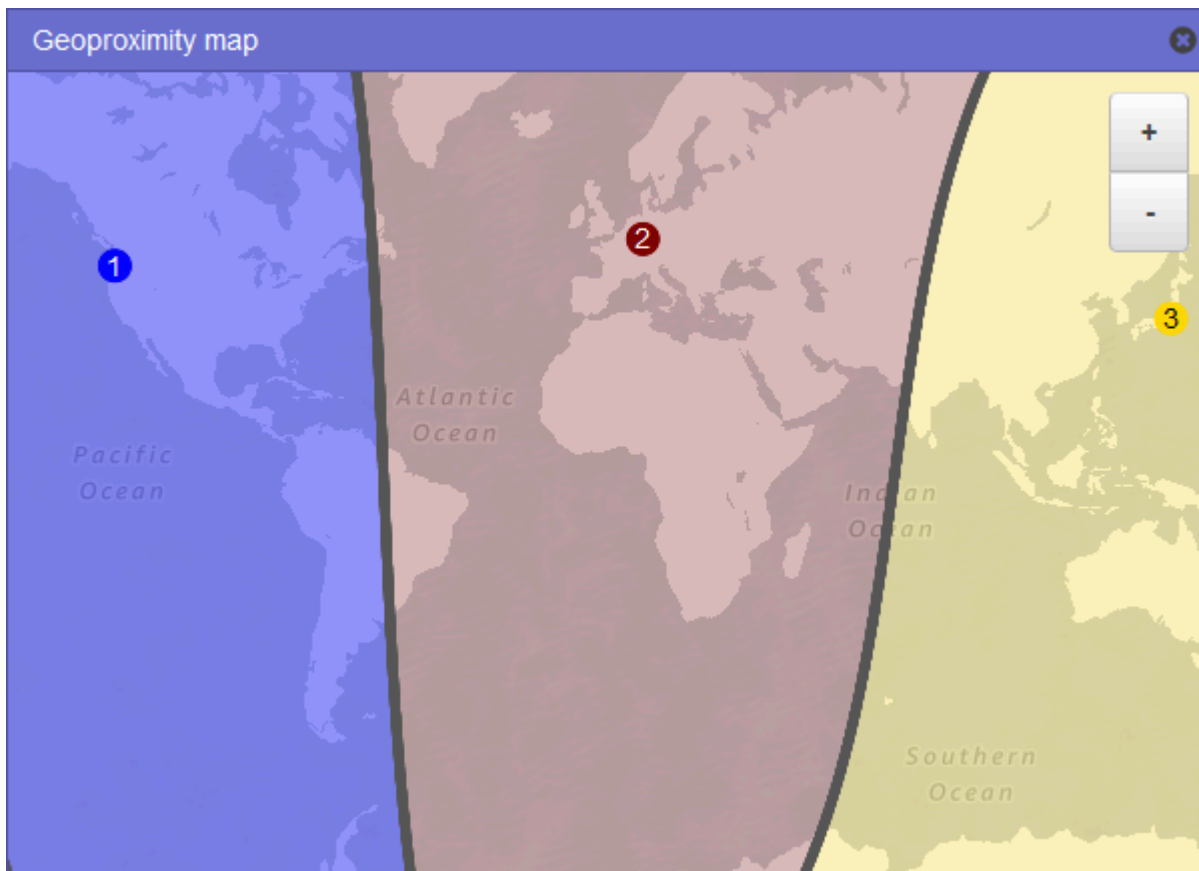
Peta untuk aturan geoproximity secara otomatis ditampilkan di Properti dan pembaruan saat Anda menambah atau menghapus wilayah.

Perhatikan hal-hal berikut:

- Peta ini akurat untuk dalam jarak sekitar 10 mil (16 kilometer).
- Peta secara otomatis menyesuaikan saat Anda menambahkan, mengedit, atau menghapus Wilayah, atau saat Anda mengubah setelan bias untuk Wilayah.
- Nomor wilayah dan warna di setiap definisi aturan sesuai dengan angka dan warna pada peta.
- Anda dapat memperbesar dan memperkecil untuk melihat lebih banyak atau lebih sedikit detail. Gunakan tombol + dan - pada peta, touchpad, atau roda pada mouse untuk mengubah tingkat zoom. Jika Anda tidak melihat Region, atau nomor Region, Anda dapat memperbesar panel Properti dan mereka akan muncul.
- Anda dapat memindahkan peta di dalam jendela peta untuk melihat area tertentu. Gunakan touchpad, atau klik dan seret peta dengan mouse. Anda juga dapat memindahkan jendela peta di jendela browser.
- Jika Anda memiliki lebih dari satu aturan geoproximity dalam suatu kebijakan, Anda dapat melihat peta hanya untuk satu aturan pada satu waktu.

Old console

Anda dapat menampilkan peta yang menunjukkan efek pengaturan geoproximity Anda saat ini. Misalnya, jika Anda memiliki sumber daya di Wilayah AS Barat (Oregon), Eropa (Frankfurt), dan Asia Pasifik (Tokyo), dan jika Anda tidak menentukan bias, peta akan terlihat seperti ini.



Untuk menampilkan peta aturan geoproximity, pilih ikon grafik di sebelah Tampilkan peta geoproximity. (Ikon ini muncul di bagian atas aturan.) Untuk menyembunyikan peta, pilih ikon lagi atau pilih X di pojok kanan atas peta.

Perhatikan hal-hal berikut:

- Peta ini akurat untuk dalam jarak sekitar 10 mil (16 kilometer).
- Peta secara otomatis menyesuaikan saat Anda menambahkan, mengedit, atau menghapus Wilayah, atau saat Anda mengubah setelan bias untuk Wilayah.
- Nomor wilayah dan warna di setiap definisi aturan sesuai dengan angka dan warna pada peta.
- Anda dapat memperbesar dan memperkecil untuk melihat lebih banyak atau lebih sedikit detail. Gunakan tombol + dan - pada peta, touchpad, atau roda pada mouse untuk mengubah tingkat zoom.
- Anda dapat memindahkan peta di dalam jendela peta untuk melihat area tertentu. Gunakan touchpad, atau klik dan seret peta dengan mouse. Anda juga dapat memindahkan jendela peta di jendela browser.

- Jika Anda memiliki lebih dari satu aturan geoproximity dalam suatu kebijakan, Anda dapat melihat peta hanya untuk satu aturan pada satu waktu.

Membuat versi tambahan dari kebijakan lalu lintas

Ketika Anda mengedit kebijakan lalu lintas, Amazon Route 53 secara otomatis membuat versi lain dari kebijakan lalu lintas dan mempertahankan versi sebelumnya kecuali Anda memilih untuk menghapusnya. Versi baru memiliki nama yang sama dengan kebijakan lalu lintas yang Anda edit; itu dibedakan dari versi aslinya dengan nomor versi yang Route 53 bertambah secara otomatis. Anda dapat mendasarkan versi baru dari kebijakan lalu lintas pada versi yang ada dari kebijakan lalu lintas yang memiliki nama yang sama.

Route 53 tidak menggunakan kembali nomor versi untuk versi baru dari kebijakan lalu lintas yang diberikan. Misalnya, jika Anda membuat tiga versi MyTrafficPolicy, menghapus dua versi terakhir, dan kemudian membuat versi lain, versi baru adalah versi 4. Dengan mempertahankan versi sebelumnya, Route 53 memastikan bahwa Anda dapat memutar kembali ke konfigurasi sebelumnya jika konfigurasi baru tidak merutekan lalu lintas seperti yang Anda inginkan.

Untuk membuat versi kebijakan lalu lintas, lakukan prosedur berikut ini.

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk membuat versi lain dari kebijakan lalu lintas

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).

3. Pilih nama kebijakan lalu lintas yang ingin Anda buat versi baru.
4. Di tabel Versi kebijakan lalu lintas di bagian atas halaman, pilih kotak centang untuk versi kebijakan lalu lintas yang ingin Anda gunakan sebagai dasar untuk versi kebijakan lalu lintas baru.
5. Pilih Edit policy as new version (Edit kebijakan sebagai versi baru).
6. Pada kotak dialog Edit kebijakan sebagai versi baru, masukkan deskripsi untuk versi kebijakan lalu lintas baru. Kami menyarankan Anda menentukan deskripsi yang membedakan versi ini dari versi lain dari kebijakan lalu lintas yang sama. Ketika Anda membuat catatan kebijakan baru, nilai yang Anda tentukan muncul dalam daftar versi yang tersedia untuk kebijakan lalu lintas ini.
7. Pilih Berikutnya.
8. Memperbarui konfigurasi yang berlaku. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).

Anda dapat menghapus aturan, titik akhir, dan cabang kebijakan lalu lintas dengan cara berikut:

- Untuk menghapus aturan atau titik akhir, pilih di editor dan kemudian pilih Hapus di panel Properti.

 Important

Jika Anda menghapus aturan yang memiliki aturan turunan dan titik akhir, Route 53 juga menghapus semua turunan.

- Jika Anda menghubungkan dua aturan ke aturan anak atau titik akhir yang sama dan Anda ingin menghapus salah satu koneksi, pilih koneksi yang ingin Anda hapus, lalu pilih Hapus di panel Properti.
9. Setelah selesai mengedit, pilih Save as new version (Simpan sebagai versi baru).
 10. Opsional: Tentukan pengaturan untuk membuat satu atau lebih catatan kebijakan di satu zona yang di-hosting dengan menggunakan versi kebijakan lalu lintas baru. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#). Anda juga dapat membuat catatan kebijakan nanti, baik di zona yang di-hosting yang sama atau di zona yang di-hosting tambahan.

Jika Anda tidak ingin membuat catatan kebijakan sekarang, pilih Batal, dan konsol akan menampilkan daftar kebijakan lalu lintas dan catatan kebijakan yang telah Anda buat menggunakan AWS akun saat ini.

11. Jika Anda menetapkan pengaturan untuk catatan kebijakan di langkah sebelumnya, pilih Create policy record (Buat catatan kebijakan).

Old console

Untuk membuat versi lain dari kebijakan lalu lintas

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
3. Pilih nama kebijakan lalu lintas yang ingin Anda buat versi baru.
4. Di tabel Versi kebijakan lalu lintas di bagian atas halaman, pilih kotak centang untuk versi kebijakan lalu lintas yang ingin Anda gunakan sebagai dasar untuk versi kebijakan lalu lintas baru.
5. Pilih Edit policy as new version (Edit kebijakan sebagai versi baru).
6. Di halaman Perbarui deskripsi, masukkan deskripsi untuk versi kebijakan lalu lintas baru. Kami menyarankan Anda menentukan deskripsi yang membedakan versi ini dari versi lain dari kebijakan lalu lintas yang sama. Ketika Anda membuat catatan kebijakan baru, nilai yang Anda tentukan muncul dalam daftar versi yang tersedia untuk kebijakan lalu lintas ini.
7. Pilih Berikutnya.
8. Memperbarui konfigurasi yang berlaku. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).

Anda dapat menghapus aturan, titik akhir, dan cabang kebijakan lalu lintas dengan cara berikut:

- Untuk menghapus aturan atau titik akhir, klik x di sudut kanan atas kotak.

Important

Jika Anda menghapus aturan yang memiliki aturan turunan dan titik akhir, Route 53 juga menghapus semua turunan.

- Jika Anda menyambungkan dua aturan ke aturan turunan atau titik akhir yang sama dan Anda ingin menghapus salah satu koneksi, jeda kursor Anda pada koneksi yang ingin Anda hapus, dan klik x untuk koneksi tersebut.
9. Setelah selesai mengedit, pilih Save as new version (Simpan sebagai versi baru).
 10. Opsional: Tentukan pengaturan untuk membuat satu atau lebih catatan kebijakan di satu zona yang di-hosting dengan menggunakan versi kebijakan lalu lintas baru. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#). Anda juga dapat membuat catatan kebijakan nanti, baik di zona yang di-hosting yang sama atau di zona yang di-hosting tambahan.

Jika Anda tidak ingin membuat catatan kebijakan sekarang, pilih Lewati langkah ini, dan konsol akan menampilkan daftar kebijakan lalu lintas dan catatan kebijakan yang telah Anda buat menggunakan AWS akun saat ini.

11. Jika Anda menetapkan pengaturan untuk catatan kebijakan di langkah sebelumnya, pilih Create policy record (Buat catatan kebijakan).

Membuat kebijakan lalu lintas dengan menggunakan dokumen JSON

Anda dapat membuat kebijakan lalu lintas baru atau versi baru dari kebijakan lalu lintas yang ada dengan mengimpor dokumen dalam format JSON yang menjelaskan semua titik akhir dan aturan yang ingin Anda sertakan dalam kebijakan lalu lintas. Untuk informasi tentang format dokumen JSON dan beberapa contoh yang dapat Anda salin dan revisi, lihat [Format dokumen kebijakan lalu lintas](#) dalam Referensi API Amazon Route 53.

Cara termudah untuk mendapatkan dokumen berformat JSON untuk versi kebijakan lalu lintas yang ada adalah dengan menggunakan perintah `get-traffic-policy` di CLI. AWS Untuk informasi selengkapnya, lihat [get-traffic-policy](#) dalam AWS CLI Referensi Perintah.

File JSON yang dibuat oleh `get-traffic-policy` perintah termasuk garis miring mundur (`\`) sebagai karakter escape. Sebelum Anda mengimpor file JSON, ganti semua garis miring mundur dengan karakter null.

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk membuat kebijakan lalu lintas dengan mengimpor dokumen JSON

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Untuk membuat kebijakan lalu lintas baru dengan mengimpor dokumen JSON, lakukan langkah-langkah berikut:
 - a. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
 - b. Pilih Create traffic policy (Buat kebijakan lalu lintas).
 - c. Pada halaman Kebijakan nama, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).
 - d. Lewati ke langkah 4.
3. Untuk membuat versi baru dari kebijakan lalu lintas yang ada dengan mengimpor dokumen JSON, lakukan langkah-langkah berikut:
 - a. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
 - b. Pilih nama kebijakan lalu lintas yang ingin Anda gunakan sebagai dasar versi baru.
 - c. Pada tabel Versi kebijakan lalu lintas, pilih kotak centang untuk versi yang ingin Anda gunakan untuk mendasarkan versi baru.
 - d. Pilih Edit policy as new version (Edit kebijakan sebagai versi baru).
 - e. Pada halaman Perbarui deskripsi, masukkan deskripsi untuk versi baru.
 - f. Lewati ke langkah 4.
4. Pilih Berikutnya.
5. Pada halaman editor pilih ikon json editor



di sudut kanan atas editor.

6. Masukkan kebijakan lalu lintas baru, tempelkan contoh kebijakan lalu lintas, atau tempelkan kebijakan lalu lintas yang ada.

Misalnya kebijakan, lihat [contoh JSON kebijakan Arus Lalu Lintas](#).

7. Pilih Perbarui.

Old console

Untuk membuat kebijakan lalu lintas dengan mengimpor dokumen JSON

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Untuk membuat kebijakan lalu lintas baru dengan mengimpor dokumen JSON, lakukan langkah-langkah berikut:
 - a. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
 - b. Pilih Create traffic policy (Buat kebijakan lalu lintas).
 - c. Pada halaman Kebijakan nama, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai-nilai yang Anda tentukan ketika Anda membuat kebijakan lalu lintas](#).
 - d. Lewati ke langkah 4.
3. Untuk membuat versi baru dari kebijakan lalu lintas yang ada dengan mengimpor dokumen JSON, lakukan langkah-langkah berikut:
 - a. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
 - b. Pilih nama kebijakan lalu lintas yang ingin Anda gunakan sebagai dasar versi baru.
 - c. Pada tabel Versi kebijakan lalu lintas, pilih kotak centang untuk versi yang ingin Anda gunakan untuk mendasarkan versi baru.
 - d. Pilih Edit policy as new version (Edit kebijakan sebagai versi baru).
 - e. Pada halaman Perbarui deskripsi, masukkan deskripsi untuk versi baru.
 - f. Lewati ke langkah 4.
4. Pilih Berikutnya.
5. Pilih Import traffic policy (Impor kebijakan lalu lintas).
6. Masukkan kebijakan lalu lintas baru, tempelkan contoh kebijakan lalu lintas, atau tempelkan kebijakan lalu lintas yang ada.

Misalnya kebijakan, lihat Contoh [JSON kebijakan Arus Lalu Lintas](#)

7. Pilih Import traffic policy (Impor kebijakan lalu lintas).

Melihat versi kebijakan lalu lintas dan catatan kebijakan terkait

Anda dapat melihat semua versi yang telah dibuat untuk kebijakan lalu lintas serta semua catatan kebijakan yang Anda buat dengan menggunakan setiap versi kebijakan lalu lintas.

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk melihat versi kebijakan lalu lintas dan catatan kebijakan terkait

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
3. Pilih nama terkait kebijakan lalu lintas.
4. Daftar tabel teratas mencantumkan semua versi yang Anda buat dari kebijakan lalu lintas. Tabel tersebut mencakup informasi berikut:

Nomor versi

Jumlah setiap versi kebijakan lalu lintas yang Anda buat. Jika Anda memilih nomor versi, konsol akan menampilkan konfigurasi untuk versi tersebut.

Jumlah catatan kebijakan

Jumlah catatan kebijakan yang Anda buat menggunakan versi kebijakan lalu lintas ini.

Tipe DNS

Tipe DNS yang Anda tentukan ketika Anda membuat versi kebijakan lalu lintas.

Deskripsi versi

Deskripsi yang Anda tentukan ketika Anda membuat versi kebijakan lalu lintas.

5. Tabel bawah mencantumkan semua catatan kebijakan yang Anda buat dengan menggunakan versi kebijakan lalu lintas di bagian atas tabel. Tabel tersebut mencakup informasi berikut:

Nama DNS

Nama DNS yang Anda kaitkan dengan kebijakan lalu lintas.

Status

Kemungkinan nilainya mencakup berikut ini:

Terapan

Route 53 telah selesai membuat atau memperbarui catatan kebijakan dan catatan yang sesuai.

Membuat

Route 53 menciptakan catatan untuk catatan kebijakan baru.

Memperbarui

Anda telah memperbarui catatan kebijakan dan Route 53 dalam proses menciptakan grup baru catatan yang akan menggantikan grup catatan yang ada untuk nama DNS tertentu.

Menghapus

Route 53 dalam proses menghapus catatan kebijakan dan catatan terkait.

Gagal

Route 53 tidak dapat membuat atau memperbarui catatan kebijakan dan catatan terkait.

Tipe DNS

Tipe DNS dari semua catatan yang dibuat Route 53 untuk catatan kebijakan ini. Saat Anda mengedit catatan kebijakan, Anda harus menentukan versi kebijakan lalu lintas yang memiliki tipe DNS yang sama dengan tipe DNS untuk catatan kebijakan yang sedang Anda edit.

Versi

Menunjukkan versi kebijakan lalu lintas yang Anda gunakan untuk membuat catatan kebijakan.

TTL (dalam detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih panjang (misalnya, 172.800 detik, atau dua hari), Anda membayar lebih sedikit untuk layanan Route 53 karena resolver rekursif mengirim permintaan ke Route 53 lebih jarang. Namun, dibutuhkan waktu lebih lama untuk perubahan catatan (misalnya, alamat IP baru) untuk mengambil efek karena resolver rekursif menggunakan nilai-nilai dalam cache mereka untuk jangka waktu yang lebih lama dibandingkan meminta Route 53 untuk informasi terbaru.

Old console

Untuk melihat versi kebijakan lalu lintas dan catatan kebijakan terkait

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
3. Pilih nama kebijakan lalu lintas.
4. Daftar tabel teratas mencantumkan semua versi yang Anda buat dari kebijakan lalu lintas. Tabel tersebut mencakup informasi berikut:

Nomor versi

Jumlah setiap versi kebijakan lalu lintas yang Anda buat. Jika Anda memilih nomor versi, konsol akan menampilkan konfigurasi untuk versi tersebut.

Jumlah catatan kebijakan

Jumlah catatan kebijakan yang Anda buat menggunakan versi kebijakan lalu lintas ini.

Tipe DNS

Tipe DNS yang Anda tentukan ketika Anda membuat versi kebijakan lalu lintas.

Deskripsi versi

Deskripsi yang Anda tentukan ketika Anda membuat versi kebijakan lalu lintas.

5. Tabel bawah mencantumkan semua catatan kebijakan yang Anda buat dengan menggunakan versi kebijakan lalu lintas di bagian atas tabel. Tabel tersebut mencakup informasi berikut:

Nama DNS catatan kebijakan

Nama DNS yang Anda kaitkan dengan kebijakan lalu lintas.

Status

Kemungkinan nilainya mencakup berikut ini:

Terapan

Route 53 telah selesai membuat atau memperbarui catatan kebijakan dan catatan yang sesuai.

Membuat

Route 53 menciptakan catatan untuk catatan kebijakan baru.

Memperbarui

Anda telah memperbarui catatan kebijakan dan Route 53 dalam proses menciptakan grup baru catatan yang akan menggantikan grup catatan yang ada untuk nama DNS tertentu.

Menghapus

Route 53 dalam proses menghapus catatan kebijakan dan catatan terkait.

Gagal

Route 53 tidak dapat membuat atau memperbarui catatan kebijakan dan catatan terkait.

Versi yang digunakan

Menunjukkan versi kebijakan lalu lintas yang Anda gunakan untuk membuat catatan kebijakan.

Tipe DNS

Tipe DNS dari semua catatan yang dibuat Route 53 untuk catatan kebijakan ini. Saat Anda mengedit catatan kebijakan, Anda harus menentukan versi kebijakan lalu lintas yang memiliki tipe DNS yang sama dengan tipe DNS untuk catatan kebijakan yang sedang Anda edit.

TTL (dalam detik)

Jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih panjang (misalnya, 172.800 detik, atau dua hari), Anda membayar lebih sedikit untuk layanan Route 53 karena resolver rekursif mengirim permintaan ke Route 53 lebih jarang. Namun, dibutuhkan waktu lebih lama untuk perubahan catatan (misalnya, alamat IP baru) untuk mengambil efek karena resolver rekursif menggunakan nilai-nilai dalam cache mereka untuk jangka waktu yang lebih lama dibandingkan meminta Route 53 untuk informasi terbaru.

Menghapus versi kebijakan lalu lintas dan kebijakan lalu lintas

Untuk menghapus kebijakan lalu lintas, Anda harus menghapus semua versi (termasuk yang asli) yang telah Anda buat untuk kebijakan lalu lintas. Selain itu, untuk menghapus versi kebijakan lalu lintas, Anda harus menghapus semua catatan kebijakan yang Anda buat dengan menggunakan versi kebijakan lalu lintas.

Important

Jika Anda menghapus catatan kebijakan yang Amazon Route 53 gunakan untuk menanggapi permintaan DNS, Route 53 akan berhenti merespons permintaan untuk nama DNS yang sesuai. Misalnya, jika Route 53 menggunakan catatan kebijakan untuk `www.example.com` untuk menanggapi kueri DNS untuk `www.example.com` dan Anda menghapus catatan kebijakan, pengguna Anda tidak akan dapat mengakses situs web atau aplikasi web Anda dengan menggunakan nama domain `www.example.com`.

Untuk menghapus versi kebijakan lalu lintas dan, secara opsional, kebijakan lalu lintas, lakukan prosedur berikut:

 Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk menghapus versi kebijakan lalu lintas dan kebijakan lalu lintas

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
3. Pilih nama terkait kebijakan lalu lintas yang ingin Anda hapus versi kebijakan lalu lintas dan, secara opsional, Anda ingin menghapus sepenuhnya.
4. Jika versi kebijakan lalu lintas yang ingin Anda hapus di tabel atas muncul di kolom Versi dalam tabel Catatan kebijakan, pilih kotak centang untuk catatan kebijakan terkait di tabel bawah.

Sebagai contoh, jika Anda ingin menghapus versi 3 dari kebijakan lalu lintas tetapi Anda membuat salah satu catatan kebijakan di tabel bawah dengan menggunakan versi 3, pilih kotak centang untuk catatan kebijakan tersebut.

5. Pilih Hapus catatan kebijakan dan di kotak dialog Hapus catatan kebijakan, pilih Konfirmasi.
6. Segarkan halaman hingga catatan kebijakan yang Anda hapus tidak lagi muncul di tabel.
7. Di bagian atas tabel, pilih kotak centang untuk versi kebijakan lalu lintas yang ingin Anda hapus.
8. Pilih Hapus.

9. Jika Anda menghapus semua versi kebijakan lalu lintas pada langkah sebelumnya dan Anda juga ingin menghapus kebijakan lalu lintas, segarkan halaman untuk menyegarkan tampilan hingga tabel kosong.
10. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
11. Dalam daftar kebijakan lalu lintas, pilih kotak centang untuk kebijakan lalu lintas yang ingin Anda hapus.
12. Pilih Delete traffic policy (Hapus kebijakan lalu lintas).

Old console

Untuk menghapus versi kebijakan lalu lintas dan kebijakan lalu lintas

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).
3. Pilih nama kebijakan lalu lintas yang ingin Anda hapus versi kebijakan lalu lintasnya dan yang, secara opsional, ingin Anda hapus sepenuhnya.
4. Jika versi kebijakan lalu lintas yang ingin Anda hapus dalam tabel atas muncul di kolom Versi yang digunakan di bagian bawah tabel, pilih kotak centang untuk catatan kebijakan yang sesuai di bagian bawah tabel.

Sebagai contoh, jika Anda ingin menghapus versi 3 dari kebijakan lalu lintas tetapi Anda membuat salah satu catatan kebijakan di tabel bawah dengan menggunakan versi 3, pilih kotak centang untuk catatan kebijakan tersebut.

5. Pilih Delete policy records (Hapus catatan kebijakan).
6. Pilih tombol segarkan untuk tabel bawah untuk menyegarkan tampilan hingga catatan kebijakan yang Anda hapus tidak lagi muncul di tabel.
7. Di bagian atas tabel, pilih kotak centang untuk versi kebijakan lalu lintas yang ingin Anda hapus.
8. Pilih Delete version (Hapus versi).
9. Jika Anda menghapus semua versi kebijakan lalu lintas di langkah sebelumnya dan Anda juga ingin menghapus kebijakan lalu lintas, pilih tombol segarkan untuk tabel atas untuk menyegarkan tampilan hingga tabel kosong.
10. Di panel navigasi, pilih Traffic policies (Kebijakan lalu lintas).

11. Dalam daftar kebijakan lalu lintas, pilih kotak centang untuk kebijakan lalu lintas yang ingin Anda hapus.
12. Pilih Delete traffic policy (Hapus kebijakan lalu lintas).

Membuat dan mengelola catatan kebijakan

Untuk merutekan lalu lintas internet ke sumber daya yang Anda tentukan ketika Anda membuat [kebijakan lalu lintas](#), Anda membuat satu atau lebih catatan kebijakan. Setiap catatan kebijakan mengidentifikasi zona yang di-hosting di mana Anda ingin membuat catatan kebijakan dan nama domain atau subdomain tempat Anda ingin merutekan lalu lintas. Sebagai contoh, jika Anda ingin merutekan lalu lintas untuk `www.example.com`, Anda menetapkan ID zona yang di-hosting untuk zona yang di-hosting `example.com`, dan Anda menentukan `www.example.com` untuk Nama DNS catatan kebijakan.

Jika Anda ingin menggunakan kebijakan lalu lintas yang sama untuk mengarahkan lalu lintas ke lebih dari satu domain atau nama subdomain, Anda memiliki dua opsi:

- Anda dapat membuat catatan kebijakan untuk setiap nama domain atau subdomain.
- Anda dapat membuat satu catatan kebijakan lalu membuat catatan CNAME atau alias yang merujuk ke catatan kebijakan.

Misalnya, jika Anda ingin menggunakan kebijakan lalu lintas yang sama untuk `example.com`, `example.net`, dan `example.org`, Anda dapat melakukan salah satu hal berikut:

- Buat satu catatan kebijakan untuk masing-masing catatan tersebut.
- Membuat catatan kebijakan untuk salah satu dari mereka dan kemudian membuat data CNAME di zona yang di-hosting untuk dua lainnya. Dalam dua catatan CNAME, Anda menentukan nama catatan yang Anda buat untuk catatan kebijakan.

Jika Anda ingin menggunakan kebijakan lalu lintas yang sama untuk domain dan subdomainnya, seperti `example.com` dan `www.example.com`, Anda dapat membuat rekaman kebijakan untuk satu nama, lalu membuat rekaman alias untuk sisanya. Misalnya, Anda dapat membuat catatan kebijakan untuk `example.com` dan kemudian membuat catatan alias untuk `www.example.com` yang memiliki catatan `example.com` sebagai target alias.

 Note

Ada biaya bulanan untuk setiap catatan kebijakan yang Anda buat. Jika Anda ingin menggunakan kebijakan lalu lintas yang sama untuk beberapa nama domain atau subdomain, Anda dapat menggunakan data CNAME atau alias untuk mengurangi biaya:

- Jika Anda membuat satu catatan kebijakan dan satu atau beberapa catatan CNAME yang merujuk ke catatan kebijakan, Anda hanya membayar untuk catatan kebijakan dan untuk kueri DNS untuk catatan CNAME.
- Jika Anda membuat satu catatan kebijakan dan satu atau lebih alias catatan di zona yang di-hosting yang sama yang merujuk ke catatan kebijakan, Anda membayar hanya untuk catatan kebijakan dan permintaan DNS untuk catatan alias.

Topik

- [Membuat catatan kebijakan](#)
- [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#)
- [Memperbarui catatan kebijakan](#)
- [Menghapus catatan kebijakan](#)

Membuat catatan kebijakan

Untuk membuat catatan kebijakan, lakukan prosedur berikut ini.

 Important

Untuk setiap catatan kebijakan yang Anda buat, Anda dikenakan biaya bulanan. Jika nanti Anda menghapus catatan kebijakan, biaya akan disamaratakan. Untuk informasi lebih lanjut, lihat bagian "Arus Lalu Lintas" di halaman [Harga Amazon Route 53](#).

 Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk membuat catatan kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Policy records (Catatan kebijakan).
3. Pada halaman Policy records (Catatan kebijakan), pilih Create policy records (Buat catatan kebijakan).
4. Pada halaman Buat catatan kebijakan, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#).
5. Untuk menambahkan catatan tambahan ke zona yang dihosting yang sama, Pilih Tambahkan catatan kebijakan.
6. Pilih Create policy records (Buat catatan kebijakan).

Diperlukan beberapa menit agar status catatan kebijakan yang dibuat ditampilkan sebagai Diterapkan.

7. Jika Anda ingin membuat catatan kebijakan di zona yang di-hosting lain, ulangi langkah 3 hingga 5.

Note

Jika status catatan kebijakan Gagal, pilih tombol info di sebelah status untuk mendapatkan informasi selengkapnya tentang kegagalan tersebut. Jika Anda memerlukan bantuan lebih lanjut dan ingin menghubungi AWS dukungan, lihat [Bagaimana cara mendapatkan dukungan teknis AWS?](#)

Old console

Untuk membuat catatan kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Policy records (Catatan kebijakan).
3. Pada halaman Policy records (Catatan kebijakan), pilih Create policy records (Buat catatan kebijakan).
4. Pada halaman Buat catatan kebijakan, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#).
5. Pilih Create policy records (Buat catatan kebijakan).

Diperlukan beberapa menit agar status catatan kebijakan yang dibuat ditampilkan sebagai Diterapkan.

6. Jika Anda ingin membuat catatan kebijakan di zona yang di-hosting lain, ulangi langkah 3 hingga 5.

Note

Jika status catatan kebijakan Gagal, pilih tombol info di sebelah status untuk mendapatkan informasi selengkapnya tentang kegagalan tersebut. Jika Anda memerlukan bantuan lebih lanjut dan ingin menghubungi AWS dukungan, lihat [Bagaimana cara mendapatkan dukungan teknis AWS?](#)

Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama. Daftar berikut berlaku untuk kedua konsol, kecuali jika dicatat.

Saat Anda membuat atau memperbarui catatan kebijakan, Anda menentukan nilai berikut

- [Traffic policy](#)
- [Version](#)
- [Hosted zone](#)
- [Policy record DNS name](#)
- [TTL](#)

Kebijakan lalu lintas

Pilih kebijakan lalu lintas konfigurasi yang ingin Anda gunakan untuk catatan kebijakan ini.

Versi

Pilih versi kebijakan lalu lintas konfigurasi yang ingin Anda gunakan untuk catatan kebijakan ini.

Jika Anda memperbarui catatan kebijakan yang ada, Anda harus memilih versi yang tipe DNS cocok dengan tipe DNS saat ini dari catatan kebijakan. Sebagai contoh, jika tipe DNS catatan kebijakan adalah A, Anda harus memilih versi dengan tipe DNS A.

Zona yang di-hosting

Pilih zona yang di-hosting tempat Anda ingin membuat catatan kebijakan dengan menggunakan kebijakan lalu lintas yang ditentukan dan versi. Anda tidak dapat mengubah nilai zona yang di-hosting setelah Anda membuat catatan kebijakan.

Nama DNS (konsol baru), Catatan kebijakan nama DNS (konsol lama)

Saat Anda membuat rekaman kebijakan, masukkan nama domain atau nama subdomain yang Anda inginkan agar Route 53 merespons kueri DNS dengan menggunakan konfigurasi dalam kebijakan dan versi lalu lintas yang ditentukan.

Untuk menggunakan konfigurasi yang sama untuk lebih dari satu nama domain atau nama subdomain di zona host yang ditentukan, pilih Tambahkan catatan kebijakan (konsol baru), atau Tambahkan catatan kebijakan lain (konsol lama), lalu masukkan nama domain atau nama subdomain dan TTL yang berlaku.

Anda tidak dapat mengubah nilai Nama DNS catatan kebijakan setelah Anda membuat catatan kebijakan.

TTL (dalam detik)

Masukkan jumlah waktu, dalam detik, yang Anda inginkan untuk resolver rekursif DNS untuk menyimpan informasi tentang catatan ini dalam cache. Jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda membayar lebih sedikit untuk layanan Route 53 karena resolver rekursif mengirim permintaan ke Route 53 lebih jarang. Namun, dibutuhkan waktu lebih lama untuk perubahan catatan (misalnya, alamat IP baru) untuk mengambil efek karena resolver rekursif menggunakan nilai-nilai dalam cache mereka untuk jangka waktu yang lebih lama dibandingkan meminta Route 53 untuk informasi terbaru.

Memperbarui catatan kebijakan

Untuk memperbarui pengaturan dalam catatan kebijakan, lakukan prosedur berikut ini.

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk memperbarui catatan kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Policy records (Catatan kebijakan).
3. Pada halaman Catatan kebijakan, pilih kotak centang untuk catatan kebijakan yang ingin Anda perbarui, lalu pilih Edit.
4. Pada halaman Edit catatan kebijakan, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#).

5. Pilih Edit policy record (Edit catatan kebijakan).

Diperlukan beberapa menit agar status catatan kebijakan yang dibuat ditampilkan sebagai Diterapkan.

6. Jika Anda ingin memperbarui catatan kebijakan lain, ulangi langkah 3 hingga 5.

 Note

Jika status catatan kebijakan Gagal, pilih tombol info di sebelah status untuk mendapatkan informasi selengkapnya tentang kegagalan tersebut. Jika Anda memerlukan bantuan lebih lanjut dan ingin menghubungi AWS dukungan, lihat [Bagaimana cara mendapatkan dukungan teknis AWS?](#)

Old console

Untuk memperbarui catatan kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Policy records (Catatan kebijakan).
3. Pada halaman Policy records (Catatan kebijakan), pilih kotak centang untuk catatan kebijakan yang ingin Anda perbarui, dan pilih Edit policy record (Edit catatan kebijakan).
4. Pada halaman Edit catatan kebijakan, tentukan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui catatan kebijakan](#).
5. Pilih Edit policy record (Edit catatan kebijakan).

Diperlukan beberapa menit agar status catatan kebijakan yang dibuat ditampilkan sebagai Diterapkan.

6. Jika Anda ingin memperbarui catatan kebijakan lain, ulangi langkah 3 hingga 5.

 Note

Jika status catatan kebijakan Gagal, pilih tombol info di sebelah status untuk mendapatkan informasi selengkapnya tentang kegagalan tersebut. Jika Anda memerlukan

bantuan lebih lanjut dan ingin menghubungi AWS dukungan, lihat [Bagaimana cara mendapatkan dukungan teknis AWS?](#)

Menghapus catatan kebijakan

Untuk menghapus catatan kebijakan, lakukan prosedur berikut ini.

Important

Jika Anda menghapus catatan kebijakan yang Amazon Route 53 gunakan untuk menanggapi permintaan DNS, Route 53 akan berhenti merespons permintaan untuk nama DNS yang sesuai. Misalnya, jika Route 53 menggunakan catatan kebijakan untuk `www.example.com` untuk menanggapi kueri DNS untuk `www.example.com` dan Anda menghapus catatan kebijakan, pengguna Anda tidak akan dapat mengakses situs web atau aplikasi web Anda dengan menggunakan nama domain `www.example.com`.

Note

Kami memperbarui konsol Arus Lalu Lintas untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk menghapus rekaman kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Policy records (Catatan kebijakan).

3. Pada halaman Catatan kebijakan, pilih kotak centang untuk catatan kebijakan yang ingin dihapus, lalu pilih Hapus.
4. Pada kotak dialog Hapus catatan kebijakan, pilih Konfirmasi.

Tunggu beberapa menit dan segarkan halaman untuk memastikan catatan kebijakan hilang dari daftar.

Old console

Untuk menghapus rekaman kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Policy records (Catatan kebijakan).
3. Pada halaman Policy records (Catatan kebijakan), pilih kotak centang untuk catatan kebijakan yang ingin Anda perbarui, dan pilih Delete policy record (Hapus catatan kebijakan).

Tunggu beberapa menit dan segarkan halaman untuk memastikan catatan kebijakan hilang dari daftar.

Apa itu Route 53 VPC Resolver?

Route 53 VPC Resolver merespons secara rekursif kueri DNS dari sumber daya AWS untuk catatan publik, nama DNS khusus Amazon VPC, dan zona host pribadi Amazon Route 53, dan tersedia secara default di semua VPCs

Note

Route 53 VPC Resolver sebelumnya disebut Route 53 Resolver, tetapi diganti namanya ketika Route 53 Global Resolver diperkenalkan.

VPC Amazon terhubung ke Resolver VPC di alamat IP VPC+2. Alamat VPC+2 ini terhubung ke Resolver VPC dalam Availability Zone.

Resolver VPC secara otomatis menjawab kueri DNS untuk:

- Nama domain VPC lokal untuk instans EC2 (misalnya, ec2-192-0-2-44.compute-1.amazonaws.com).
- Rekaman di zona yang dihosting pribadi (misalnya, acme.example.com).
- Untuk nama domain publik, VPC Resolver melakukan pencarian rekursif terhadap server nama publik di internet.

Jika Anda memiliki beban kerja yang memanfaatkan sumber daya lokal VPCs dan sumber daya lokal, Anda juga perlu menyelesaikan catatan DNS yang dihosting di lokasi. Demikian pula, sumber daya lokal ini mungkin perlu menyelesaikan nama yang dihosting. AWS Melalui titik akhir Resolver dan aturan penerusan bersyarat, Anda dapat menyelesaikan kueri DNS antara sumber daya lokal dan VPCs membuat pengaturan cloud hybrid melalui VPN atau Direct Connect (DX). Secara khusus:

- Titik akhir Inbound Resolver memungkinkan kueri DNS ke VPC Anda dari jaringan lokal atau VPC lain.
- Titik akhir Outbound Resolver memungkinkan kueri DNS dari VPC ke jaringan lokal atau VPC lain.
- Aturan penyelesai memungkinkan Anda membuat satu aturan penerusan untuk setiap nama domain dan menentukan nama domain yang ingin Anda teruskan kueri DNS dari VPC ke resolver

DNS lokal dan dari lokal ke VPC Anda. Aturan diterapkan langsung ke VPC Anda dan dapat dibagikan di beberapa akun.

Diagram berikut menunjukkan resolusi DNS hybrid dengan titik akhir Resolver. Perhatikan bahwa diagram disederhanakan untuk menampilkan hanya satu Availability Zone.

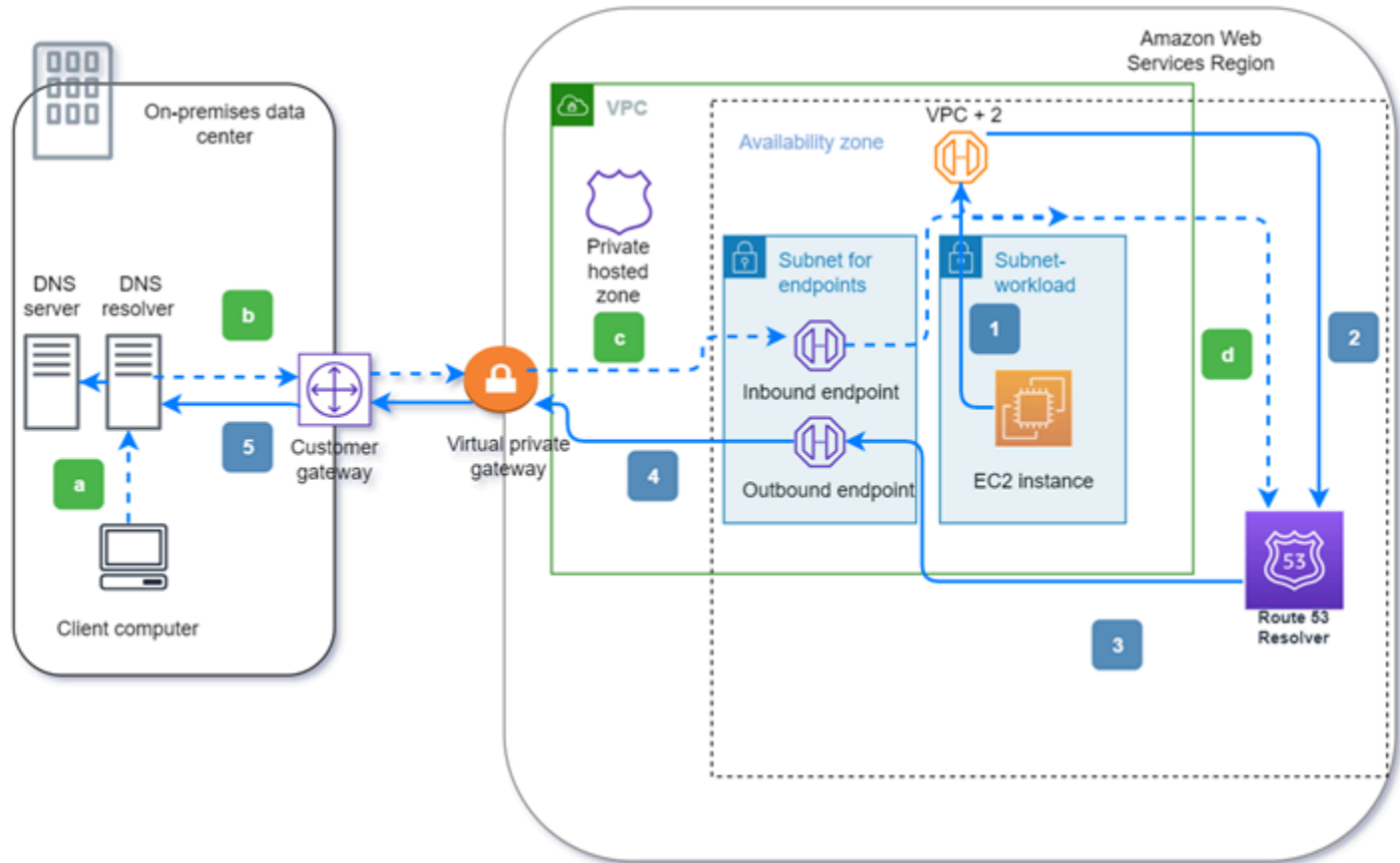


Diagram ini menggambarkan langkah-langkah berikut:

Keluar (panah padat 1—5):

1. Instans Amazon EC2 perlu menyelesaikan kueri DNS ke domain `internal.example.com`. Server DNS otoritatif berada di pusat data lokal. Kueri DNS ini dikirim ke VPC+2 di VPC yang terhubung ke VPC Resolver.
2. Aturan penerusan VPC Resolver dikonfigurasi untuk meneruskan kueri ke `internal.example.com` di pusat data lokal.
3. Kueri diteruskan ke titik akhir keluar.

4. Titik akhir keluar meneruskan kueri ke resolver DNS lokal melalui koneksi pribadi antara dan pusat data. AWS Koneksi dapat berupa Direct Connect atau AWS Site-to-Site VPN, digambarkan sebagai gateway pribadi virtual.
5. Penyelesai DNS lokal menyelesaikan kueri DNS untuk internal.example.com dan mengembalikan jawaban ke instans Amazon EC2 melalui jalur yang sama secara terbalik.

Masuk (panah putus-putus a—d):

- a. Klien di pusat data lokal perlu menyelesaikan kueri DNS ke AWS sumber daya untuk domain dev.example.com. Ini mengirimkan kueri ke resolver DNS lokal.
- b. Penyelesai DNS lokal memiliki aturan penerusan yang mengarahkan kueri ke dev.example.com ke titik akhir masuk.
- c. Kueri tiba di titik akhir masuk melalui koneksi pribadi, seperti Direct Connect atau AWS Site-to-Site VPN, digambarkan sebagai gateway virtual.
- d. Titik akhir masuk mengirimkan kueri ke VPC Resolver, dan VPC Resolver menyelesaikan kueri DNS untuk dev.example.com dan mengembalikan jawaban ke klien melalui jalur yang sama secara terbalik.

Topik

- [Menyelesaikan kueri DNS antara VPCs dan jaringan Anda](#)
- [Ketersediaan dan penskalaan Route 53 VPC Resolver](#)
- [Mulai menggunakan Route 53 VPC Resolver](#)
- [Meneruskan kueri DNS masuk ke VPCs](#)
- [Meneruskan kueri DNS keluar ke jaringan Anda](#)
- [Tutorial aturan delegasi penyelesai](#)
- [Mengaktifkan validasi DNSSEC di Amazon Route 53](#)

Menyelesaikan kueri DNS antara VPCs dan jaringan Anda

Resolver VPC berisi titik akhir yang Anda konfigurasi untuk menjawab kueri DNS ke dan dari lingkungan lokal Anda.

 Note

Meneruskan kueri DNS pribadi ke alamat VPC CIDR+2 apa pun dari server DNS VPC lokal atau lainnya tidak didukung, dan dapat menyebabkan hasil yang tidak stabil. Sebagai gantinya, kami menyarankan Anda menggunakan titik akhir masuk Resolver.

Anda juga dapat mengintegrasikan resolusi DNS antara VPC Resolver dan DNS resolver di jaringan Anda dengan mengonfigurasi aturan penerusan. Jaringan Anda dapat mencakup jaringan yang dapat dijangkau dari VPC, seperti berikut ini:

- VPC itu sendiri
- VPC lain yang tersambung
- Jaringan lokal yang terhubung AWS dengan Direct Connect, VPN, atau gateway terjemahan alamat jaringan (NAT)

Sebelum Anda mulai meneruskan kueri, Anda membuat titik akhir and/or keluar masuk Resolver di VPC yang terhubung. Titik akhir ini menyediakan jalan untuk kueri masuk atau keluar:

Titik akhir masuk: DNS resolver di jaringan Anda dapat meneruskan kueri DNS ke Route 53 VPC Resolver melalui titik akhir ini

Ada dua jenis titik akhir masuk, titik akhir masuk default yang diteruskan ke alamat IP, dan titik akhir masuk delegasi yang mendelegasikan otoritas untuk subdomain yang dihosting di Zona host pribadi Route 53 ke Resolver VPC Route 53. Titik akhir masuk memungkinkan resolver DNS Anda untuk dengan mudah menyelesaikan nama domain untuk AWS sumber daya seperti instans EC2 atau catatan di zona host pribadi Route 53. Untuk informasi selengkapnya, lihat [Bagaimana DNS resolver di jaringan Anda meneruskan kueri DNS ke titik akhir Resolver](#).

Titik akhir keluar: VPC Resolver meneruskan kueri secara kondisional ke resolver di jaringan Anda melalui titik akhir ini

Untuk meneruskan kueri yang dipilih, buat aturan Resolver yang menentukan nama domain bagi kueri DNS yang ingin Anda teruskan (misalnya example.com), dan alamat IP DNS resolver di jaringan yang menjadi tujuan penerusan permintaan. Jika kueri cocok dengan beberapa aturan (example.com, acme.example.com), VPC Resolver memilih aturan dengan kecocokan paling spesifik (acme.example.com) dan meneruskan kueri ke alamat IP yang Anda tentukan dalam

aturan tersebut. Ada tiga jenis aturan, maju, sistem, dan delegasi. Untuk informasi selengkapnya, lihat [Bagaimana titik akhir Resolver meneruskan kueri DNS dari Anda ke jaringan Anda VPCs](#).

Seperti Amazon VPC, VPC Resolver bersifat regional. Di setiap wilayah yang Anda miliki VPCs, Anda dapat memilih apakah akan meneruskan kueri dari jaringan Anda VPCs ke jaringan Anda (kueri keluar), dari jaringan Anda ke VPCs (kueri masuk), atau keduanya.

Anda tidak dapat membuat titik akhir Resolver di VPC yang tidak Anda miliki. Hanya pemilik VPC yang dapat membuat sumber daya tingkat VPC seperti titik akhir masuk.

 Note

Ketika membuat titik akhir Resolver, Anda tidak dapat menentukan VPC dengan atribut penghunian instans yang diatur ke `dedicated`. Untuk informasi selengkapnya, lihat .

Untuk menggunakan penerusan masuk atau keluar, buatlah titik akhir Resolver di VPC Anda. Sebagai bagian dari definisi titik akhir, Anda menentukan alamat IP, atau delegasi DNS, yang ingin Anda teruskan kueri DNS masuk atau alamat IP yang Anda inginkan dari kueri keluar. Untuk setiap alamat IP dan delegasi yang Anda tentukan, VPC Resolver secara otomatis membuat VPC elastic network interface.

Diagram berikut menunjukkan jalur kueri DNS dari penyelesai DNS di jaringan Anda ke titik akhir Route 53 Resolver.

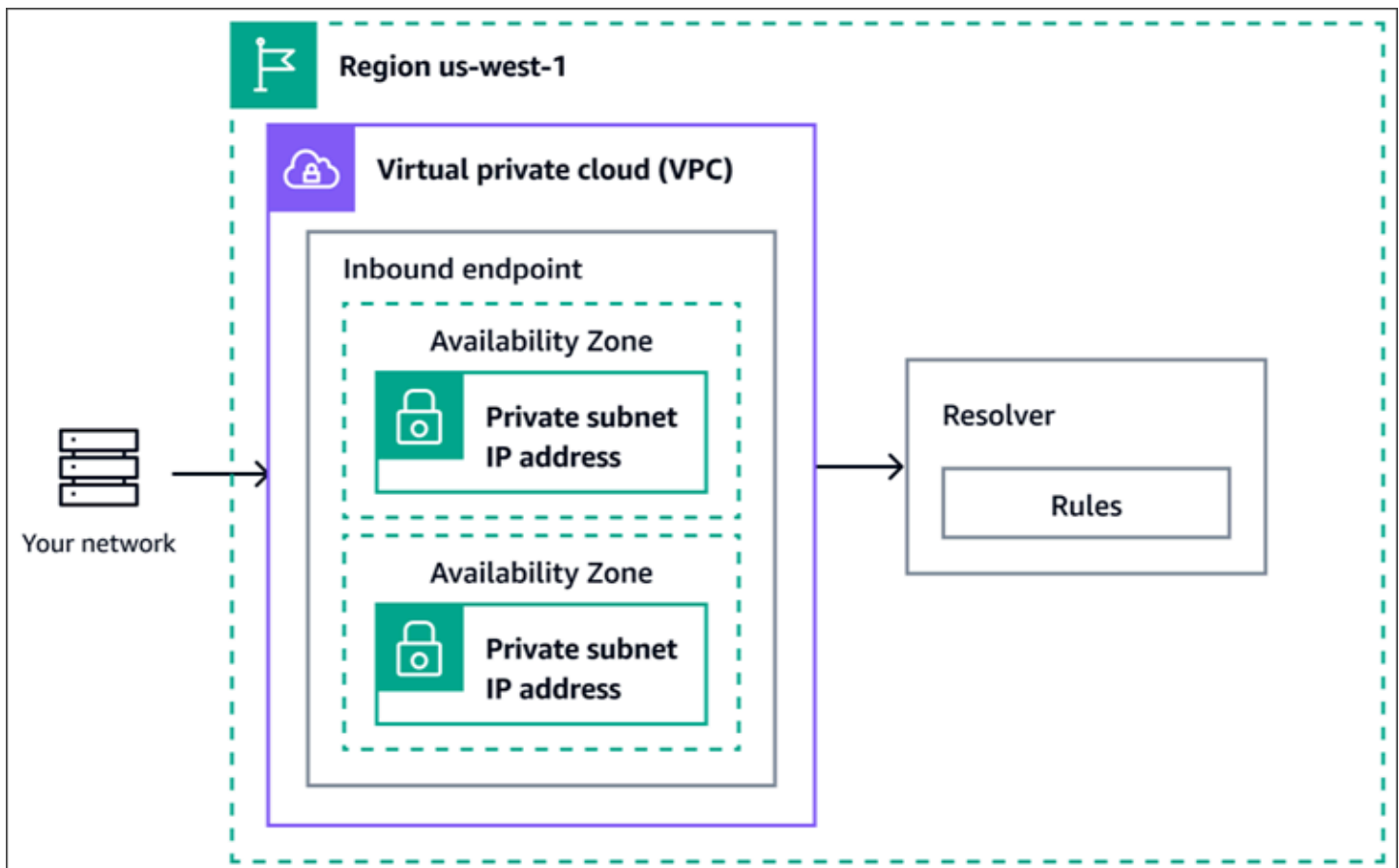
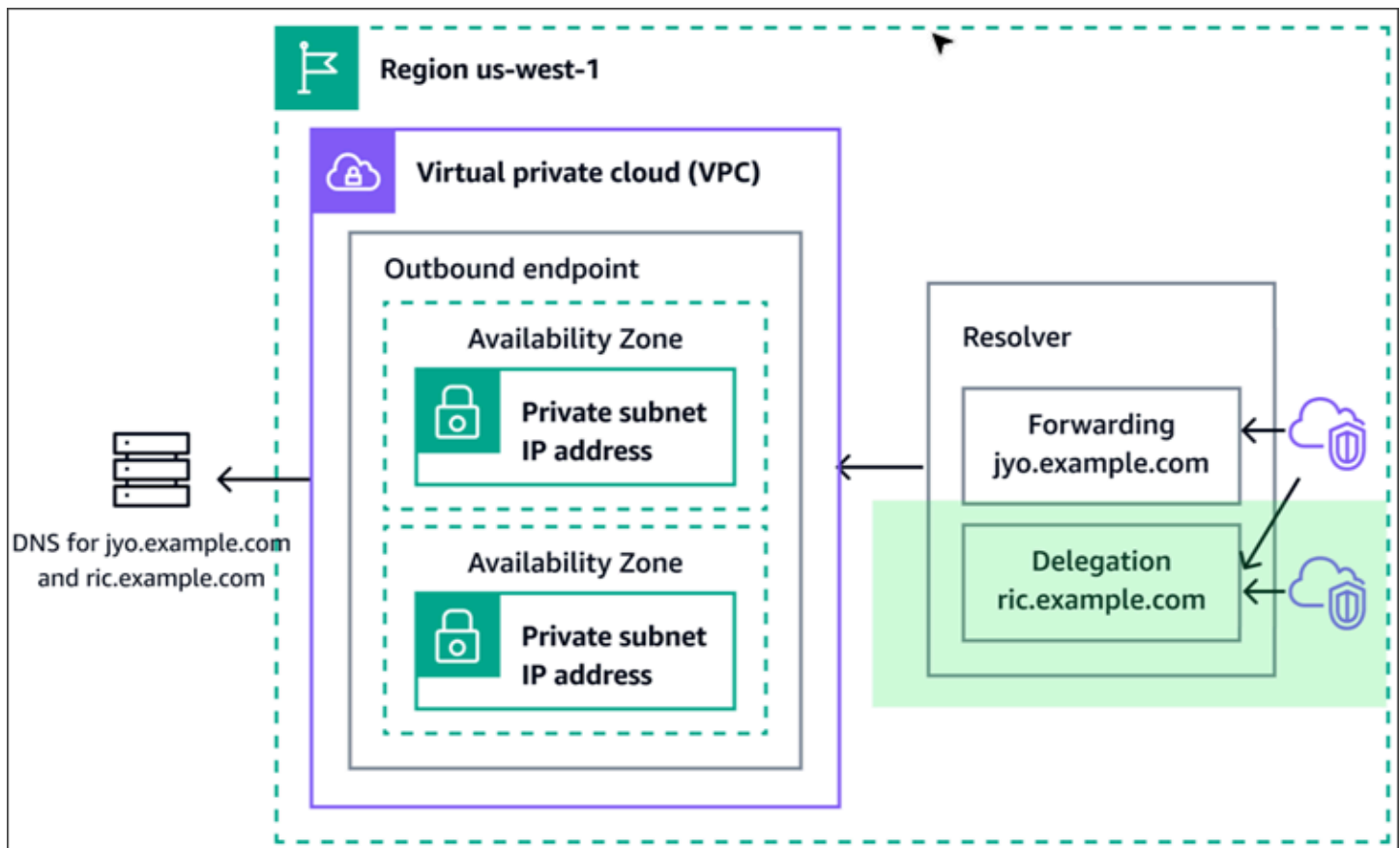


Diagram berikut menunjukkan jalur kueri DNS dari instans EC2 di salah satu resolver DNS Anda VPCs ke jaringan Anda. Domain `jyo.example.com` menggunakan aturan penerusan, sedangkan subdomain `ric.example.com` telah mendelegasikan otoritas penerusan ke VPC Resolver.



Untuk gambaran umum antarmuka jaringan VPC, lihat [Antarmuka Jaringan Elastis](#) dalam Panduan Pengguna Amazon VPC.

Topik

- [Bagaimana DNS resolver di jaringan Anda meneruskan kueri DNS ke titik akhir Resolver](#)
- [Bagaimana titik akhir Resolver meneruskan kueri DNS dari Anda ke jaringan Anda VPCs](#)
- [Pertimbangan saat membuat titik akhir masuk dan keluar](#)

Bagaimana DNS resolver di jaringan Anda meneruskan kueri DNS ke titik akhir Resolver

Untuk meneruskan kueri DNS dari jaringan Anda ke Route 53 VPC Resolver, Anda membuat titik akhir masuk di Wilayah. AWS Ada dua kategori titik akhir inbound, default dan delegasi.

Langkah-langkah untuk membuat titik akhir masuk default

1. Anda membuat titik akhir masuk Resolver default di VPC dan menentukan alamat IP tempat resolver di jaringan Anda meneruskan kueri DNS, bersama dengan grup keamanan VPC yang menyertakan aturan masuk yang memungkinkan akses TCP dan UDP pada port 53. Untuk instruksi lihat [Mengonfigurasi penerusan masuk](#).

Untuk setiap alamat IP yang Anda tentukan untuk titik akhir masuk, VPC Resolver membuat VPC elastic network interface di VPC tempat Anda membuat endpoint masuk.

2. Anda mengonfigurasi penyelesai pada jaringan guna meneruskan kueri DNS untuk nama domain yang ada ke alamat IP yang Anda tentukan di titik akhir masuk. Untuk informasi selengkapnya, lihat [Pertimbangan saat membuat titik akhir masuk dan keluar](#).

Berikut cara VPC Resolver menyelesaikan kueri DNS yang berasal dari jaringan Anda melalui titik akhir masuk default:

1. Browser web atau aplikasi lain di jaringan Anda mengirimkan kueri DNS untuk nama domain yang Anda teruskan ke VPC Resolver.
2. Penyelesai di jaringan Anda meneruskan kueri ke alamat IP di titik akhir masuk.
3. Titik akhir masuk meneruskan kueri ke VPC Resolver.
4. VPC Resolver mendapatkan nilai yang berlaku untuk nama domain dalam kueri DNS, baik secara internal atau dengan melakukan pencarian rekursif terhadap server nama publik.
5. VPC Resolver mengembalikan nilai ke titik akhir masuk.
6. Titik akhir masuk mengembalikan nilai ke penyelesai di jaringan Anda.
7. Penyelesai di jaringan Anda mengembalikan nilai ke aplikasi.
8. Menggunakan nilai yang dikembalikan oleh VPC Resolver, aplikasi mengirimkan permintaan, misalnya, permintaan untuk objek di bucket Amazon S3.

Langkah-langkah untuk membuat titik akhir masuk delegasi

1. Anda membuat titik akhir masuk Resolver delegasi di VPC. Untuk instruksi lihat [Mengonfigurasi penerusan masuk](#).

Untuk setiap alamat IP yang Anda tentukan untuk titik akhir masuk, VPC Resolver membuat VPC elastic network interface di VPC tempat Anda membuat endpoint masuk.

2. Anda mengonfigurasi resolver di jaringan Anda untuk mendelegasikan kueri DNS untuk nama domain yang berlaku ke VPC Resolver. Untuk catatan lain Anda harus memasukkan alamat IP

untuk titik akhir masuk. Untuk informasi selengkapnya, lihat [Pertimbangan saat membuat titik akhir masuk dan keluar](#).

Berikut cara VPC Resolver menyelesaikan kueri DNS yang berasal dari jaringan Anda melalui titik akhir masuk delegasi:

1. Sebagai prasyarat, Anda harus mendelegasikan subdomain yang dihosting di zona host pribadi dari lokal. Karena Anda mendelegasikan subdomain melalui titik akhir delegasi masuk, Anda menggunakan alamat IP titik akhir masuk sebagai catatan lem untuk subdomain yang didelegasikan.

 Note

Anda mungkin juga perlu menyertakan catatan lem untuk memastikan kueri DNS dapat diselesaikan. Jika Anda mendelegasikan subdomain ke server nama yang berada di zona yang sama dengan domain induk, catatan lem diperlukan.

2. Browser web atau aplikasi lain di jaringan Anda mengirimkan kueri DNS untuk nama domain yang Anda delegasikan ke Resolver VPC.
3. Penyelesai di jaringan Anda meneruskan kueri ke alamat IP di titik akhir masuk.
4. Titik akhir masuk mendelegasikan kueri ke VPC Resolver.
5. VPC Resolver mengembalikan alamat ke AWS sumber daya dari zona host pribadi ke titik akhir masuk.
6. Titik akhir masuk mengembalikan nilai ke penyelesai di jaringan Anda.
7. Penyelesai di jaringan Anda mengembalikan nilai ke aplikasi.
8. Menggunakan nilai yang dikembalikan oleh VPC Resolver, aplikasi mengirimkan permintaan, misalnya, permintaan untuk objek di bucket Amazon S3.

Membuat titik akhir masuk tidak mengubah perilaku Resolver VPC, itu hanya menyediakan jalur dari lokasi di luar jaringan ke VPC Resolver. AWS

Bagaimana titik akhir Resolver meneruskan kueri DNS dari Anda ke jaringan Anda VPCs

Saat Anda ingin meneruskan kueri DNS dari instans EC2 di satu atau lebih VPCs di AWS Wilayah ke jaringan Anda, Anda melakukan langkah-langkah berikut.

1. Anda membuat titik akhir keluar Resolver di VPC, dan Anda menentukan beberapa nilai:
 - VPC yang akan dilewati kueri DNS dalam perjalanan ke penyelesai di jaringan Anda.
 - [Grup keamanan VPC](#) yang menyertakan aturan keluar yang memungkinkan akses TCP dan UDP pada port 53 (atau port yang Anda gunakan untuk kueri DNS di jaringan Anda)

Untuk setiap alamat IP yang Anda tentukan untuk titik akhir keluar, VPC Resolver membuat antarmuka elastis network Amazon VPC di VPC yang Anda tentukan. Untuk informasi selengkapnya, lihat [Pertimbangan saat membuat titik akhir masuk dan keluar](#).

2. Anda membuat satu atau beberapa aturan, yang menentukan nama domain kueri DNS yang ingin Anda delegasikan ke VPC Resolver untuk diteruskan, atau ingin VPC Resolver diteruskan ke resolver di jaringan Anda. Untuk aturan penerusan, Anda juga menentukan alamat IP resolver. Untuk informasi selengkapnya, lihat [Menggunakan aturan untuk mengontrol kueri yang diteruskan ke jaringan Anda](#).
3. Anda mengaitkan setiap aturan dengan yang VPCs Anda inginkan untuk meneruskan kueri DNS ke jaringan Anda.

Menggunakan aturan untuk mengontrol kueri yang diteruskan ke jaringan Anda

Aturan mengontrol kueri DNS mana yang meneruskan titik akhir Resolver ke resolver DNS di jaringan Anda dan pertanyaan mana yang menjawab VPC Resolver itu sendiri.

Anda dapat mengategorikan aturan ke dalam beberapa cara. Salah satu caranya adalah siapa yang membuat aturan:

- Aturan yang ditentukan otomatis — VPC Resolver secara otomatis membuat aturan yang ditentukan secara otomatis dan mengaitkan aturan dengan aturan Anda. VPCs Sebagian besar aturan ini berlaku untuk nama domain AWS-spesifik yang VPC Resolver menjawab pertanyaan untuk. Untuk informasi selengkapnya, lihat [Nama domain yang VPC Resolver membuat aturan sistem yang ditentukan secara otomatis](#).
- Aturan kustom - Anda membuat aturan khusus dan mengaitkan aturan dengan VPCs. Saat ini, Anda dapat membuat dua jenis aturan kustom, aturan penerusan bersyarat, juga dikenal sebagai aturan penerusan, dan aturan delegasi. Aturan penerusan menyebabkan VPC Resolver meneruskan kueri DNS dari alamat IP Anda ke alamat IP untuk penyelesai DNS di jaringan Anda VPCs .

Jika Anda membuat aturan penerusan untuk domain yang sama dengan aturan yang ditentukan otomatis, VPC Resolver meneruskan kueri untuk nama domain tersebut ke resolver DNS di jaringan Anda berdasarkan pengaturan dalam aturan penerusan.

Aturan delegasi meneruskan kueri DNS dengan catatan delegasi dalam aturan delegasi yang cocok dengan catatan NS sebagai respons terhadap resolver di jaringan Anda.

Cara lain untuk mengategorikan aturan adalah hal yang dilakukan:

- Aturan penerusan bersyarat – Anda membuat aturan penerusan bersyarat (juga dikenal sebagai aturan penerusan) saat Anda ingin meneruskan kueri DNS untuk nama domain tertentu ke penyelesai DNS di jaringan Anda.
- Aturan sistem — Aturan sistem menyebabkan VPC Resolver secara selektif mengesampingkan perilaku yang didefinisikan dalam aturan penerusan. Saat Anda membuat aturan sistem, VPC Resolver menyelesaikan kueri DNS untuk subdomain tertentu yang akan diselesaikan oleh penyelesai DNS di jaringan Anda.

Secara default, aturan penerusan berlaku untuk nama domain dan semua subdomainnya. Jika Anda ingin meneruskan kueri untuk domain ke penyelesai di jaringan tetapi Anda tidak ingin meneruskan kueri untuk beberapa subdomain, buatlah aturan sistem untuk subdomain. Misalnya, jika Anda membuat aturan penerusan untuk `example.com` tetapi tidak ingin meneruskan kueri untuk `acme.example.com`, buatlah aturan sistem dan tentukan `acme.example.com` untuk nama domain.

- Aturan rekursif — VPC Resolver secara otomatis membuat aturan rekursif bernama Internet Resolver. Aturan ini menyebabkan Route 53 VPC Resolver bertindak sebagai resolver rekursif untuk nama domain apa pun yang tidak Anda buat aturan kustom dan VPC Resolver tidak membuat aturan yang ditentukan secara otomatis. Untuk informasi tentang cara menimpa perilaku ini, lihat "Meneruskan Semua Kueri ke Jaringan Anda" nanti dalam topik ini.

Anda dapat membuat aturan khusus yang berlaku untuk nama domain tertentu (milik Anda atau sebagian besar nama AWS domain), ke nama AWS domain publik, atau ke semua nama domain.

Meneruskan kueri untuk nama domain tertentu ke jaringan Anda

Untuk meneruskan kueri bagi nama domain tertentu, seperti `example.com`, ke jaringan Anda, buatlah aturan dan tentukan nama domain tersebut. Untuk aturan penerusan, Anda juga menentukan alamat IP resolver DNS di jaringan yang ingin Anda teruskan kueri, atau, untuk

aturan delegasi, buat catatan delegasi yang ingin Anda delegasikan wewenanganya ke resolver on-prem. Anda kemudian mengaitkan setiap aturan dengan yang VPCs Anda inginkan untuk meneruskan kueri DNS ke jaringan Anda. Misalnya, Anda dapat membuat aturan terpisah untuk example.com, example.org, dan example.net. Kemudian Anda dapat mengaitkan aturan dengan VPCs di AWS Wilayah dalam kombinasi apa pun.

Meneruskan kueri untuk amazonaws.com ke jaringan Anda

Nama domain amazonaws.com adalah nama domain publik untuk AWS sumber daya seperti instans EC2 dan bucket S3. Jika Anda ingin meneruskan kueri untuk amazonaws.com ke jaringan Anda, buat aturan, tentukan amazonaws.com untuk nama domain, dan tentukan Teruskan atau Delegasi untuk jenis aturan tergantung pada metode yang ingin Anda gunakan.

Note

VPC Resolver tidak secara otomatis meneruskan kueri DNS untuk beberapa subdomain amazonaws.com bahkan jika Anda membuat aturan penerusan untuk amazonaws.com. Untuk informasi selengkapnya, lihat [Nama domain yang VPC Resolver membuat aturan sistem yang ditentukan secara otomatis](#). Untuk informasi tentang cara menimpa perilaku ini, segera lihat "Meneruskan Semua Kueri ke Jaringan Anda" berikut.

Meneruskan semua kueri ke jaringan Anda

Jika Anda ingin meneruskan semua kueri ke jaringan Anda, Anda membuat aturan, tentukan "." (dot) untuk nama domain, dan kaitkan aturan dengan yang Anda inginkan VPCs untuk meneruskan semua kueri DNS ke jaringan Anda. VPC Resolver masih tidak meneruskan semua kueri DNS ke jaringan Anda karena menggunakan resolver DNS di luar akan merusak beberapa fungsionalitas. AWS Misalnya, beberapa nama AWS domain internal memiliki rentang alamat IP internal yang tidak dapat diakses dari luar AWS. Untuk daftar nama domain dengan kueri yang tidak diteruskan ke jaringan saat Anda membuat aturan untuk ".", lihat [Nama domain yang VPC Resolver membuat aturan sistem yang ditentukan secara otomatis](#).

Namun, aturan sistem yang ditentukan secara otomatis untuk DNS terbalik dapat dinonaktifkan, memungkinkan aturan "." untuk meneruskan semua kueri DNS terbalik ke jaringan Anda. Untuk informasi selengkapnya tentang cara menonaktifkan aturan yang ditentukan secara otomatis, lihat [Aturan penerusan untuk kueri DNS terbalik di VPC Resolver](#).

Jika Anda ingin mencoba meneruskan kueri DNS untuk semua nama domain ke jaringan, termasuk nama domain yang dikecualikan dari penerusan secara default, Anda dapat membuat aturan "." dan lakukan salah satu hal berikut ini:

- Mengatur bendera `enableDnsHostnames` untuk VPC ke `false`
- Membuat aturan untuk nama domain yang tercantum dalam [Nama domain yang VPC Resolver membuat aturan sistem yang ditentukan secara otomatis](#)

 Important

Jika Anda meneruskan semua nama domain ke jaringan Anda, termasuk nama domain yang dikecualikan VPC Resolver saat Anda membuat aturan ".", beberapa fitur mungkin berhenti berfungsi.

Bagaimana VPC Resolver menentukan apakah nama domain dalam kueri cocok dengan aturan apa pun

Route 53 VPC Resolver membandingkan nama domain dalam kueri DNS dengan nama domain dalam aturan yang terkait dengan VPC tempat kueri berasal. VPC Resolver menganggap nama domain cocok dalam kasus berikut:

- Nama domain cocok
- Nama domain dalam kueri adalah subdomain dari nama domain dalam aturan

Misalnya, jika nama domain dalam aturan adalah `acme.example.com`, VPC Resolver menganggap nama domain berikut dalam kueri DNS cocok:

- `acme.example.com`
- `zenith.acme.example.com`

Nama domain berikut tidak cocok:

- `contoh.com`
- `nadir.example.com`

Jika nama domain dalam kueri cocok dengan nama domain di lebih dari satu aturan (seperti `example.com` dan `www.example.com`), VPC Resolver merutekan kueri DNS keluar menggunakan aturan yang berisi nama domain paling spesifik (`www.example.com`).

Bagaimana VPC Resolver menentukan tempat untuk meneruskan kueri DNS

Ketika aplikasi yang berjalan pada instans EC2 di VPC mengirimkan kueri DNS, Route 53 VPC Resolver melakukan langkah-langkah berikut:

1. Resolver memeriksa nama domain dalam aturan.

Jika nama domain dalam kueri cocok dengan nama domain dalam aturan penerusan default, VPC Resolver meneruskan kueri ke alamat IP yang Anda tentukan saat Anda membuat titik akhir keluar. Titik akhir keluar kemudian meneruskan kueri ke alamat IP penyelesai pada jaringan Anda, yang ditentukan ketika Anda membuat aturan.

Jika catatan delegasi dalam respons cocok dengan aturan delegasi, maka Resolver mendelegasikan wewenang ke resolver on-prem melalui titik akhir keluar yang terkait dengan aturan delegasi.

Untuk informasi selengkapnya, lihat [Bagaimana VPC Resolver menentukan apakah nama domain dalam kueri cocok dengan aturan apa pun](#).

2. Titik akhir Resolver meneruskan kueri DNS berdasarkan pengaturan dalam aturan ".".

Jika nama domain dalam kueri tidak cocok dengan nama domain dalam aturan lain, VPC Resolver meneruskan kueri berdasarkan pengaturan di "yang ditentukan secara otomatis". aturan (titik). Aturan dot berlaku untuk semua nama domain kecuali beberapa nama domain AWS internal dan nama rekaman di zona host pribadi. Aturan ini menyebabkan VPC Resolver meneruskan kueri DNS ke server nama publik jika nama domain dalam kueri tidak cocok dengan nama apa pun dalam aturan penerusan kustom Anda. Jika Anda ingin meneruskan semua kueri ke penyelesai DNS di jaringan, buat aturan penerusan kustom, tentukan "." untuk nama domain, tentukan Penerusan untuk Jenis, dan tentukan alamat IP penyelesai tersebut.

3. VPC Resolver mengembalikan respon ke aplikasi yang mengirimkan query.

Menggunakan aturan di beberapa Wilayah

Route 53 VPC Resolver adalah layanan regional, sehingga objek yang Anda buat di satu AWS Wilayah hanya tersedia di Wilayah tersebut. Untuk menggunakan aturan yang sama di lebih dari satu Wilayah, Anda harus membuat aturan di setiap Wilayah.

AWS Akun yang membuat aturan dapat berbagi aturan dengan AWS akun lain. Untuk informasi selengkapnya, lihat [Berbagi aturan Resolver dengan AWS akun lain dan menggunakan aturan bersama](#).

Nama domain yang VPC Resolver membuat aturan sistem yang ditentukan secara otomatis

Resolver secara otomatis membuat aturan sistem yang ditentukan secara otomatis yang menentukan cara kueri untuk domain yang dipilih diselesaikan secara default:

- Untuk zona yang di-hosting privat dan nama domain khusus Amazon EC2 (seperti `compute.amazonaws.com` dan `compute.internal`), aturan yang ditentukan secara otomatis memastikan bahwa zona privat dan instans EC2 terus menyelesaikan jika Anda membuat aturan penerusan bersyarat untuk nama domain yang kurang spesifik seperti "." (dot) atau "com".
- Untuk nama domain yang dipesan publik (seperti `localhost` dan `10.in-addr.arpa`), praktik terbaik DNS merekomendasikan agar kueri dijawab secara lokal, bukan diteruskan ke server nama publik. Lihat [RFC 6303, Zona DNS yang Dilayani Secara Lokal](#).

Note

Jika Anda membuat aturan penerusan bersyarat untuk "." (dot) atau "com", kami sarankan agar Anda juga membuat aturan sistem untuk `amazonaws.com`. (Aturan sistem menyebabkan Resolver VPC menyelesaikan kueri DNS secara lokal untuk domain dan subdomain tertentu.) Membuat aturan sistem ini meningkatkan kinerja, mengurangi jumlah kueri yang diteruskan ke jaringan Anda, dan mengurangi biaya Resolver VPC.

Jika ingin menimpa aturan yang ditentukan secara otomatis, Anda dapat membuat aturan penerusan bersyarat untuk nama domain yang sama.

Anda juga dapat menonaktifkan beberapa aturan yang ditentukan secara otomatis. Untuk informasi selengkapnya, lihat [Aturan penerusan untuk kueri DNS terbalik di VPC Resolver](#).

VPC Resolver membuat aturan autodefined berikut.

Aturan untuk zona yang di-hosting privat

Untuk setiap zona host pribadi yang Anda kaitkan dengan VPC, VPC Resolver membuat aturan dan mengaitkannya dengan VPC. Jika Anda mengaitkan zona host pribadi dengan beberapa VPCs, VPC Resolver mengaitkan aturan dengan yang sama. VPCs

Aturan memiliki jenis Teruskan.

Aturan untuk berbagai nama domain AWS internal

Semua aturan untuk nama domain internal di bagian ini memiliki jenis Teruskan. VPC Resolver meneruskan kueri DNS untuk nama domain ini ke server nama otoritatif untuk VPC.

Note

VPC Resolver membuat sebagian besar aturan ini saat Anda menyetel flag `enableDnsHostnames` untuk VPC. `true` VPC Resolver membuat aturan meskipun Anda tidak menggunakan titik akhir Resolver.

VPC Resolver membuat aturan yang ditentukan otomatis berikut dan mengaitkannya dengan VPC saat Anda menyetel flag untuk VPC ke: `enableDnsHostnames true`

- *Region-name*.compute.internal, misalnya, eu-west-1.compute.internal. Wilayah us-east-1 tidak menggunakan nama domain ini.
- *Region-name*.menghitung. *amazon-domain-name*, misalnya, eu-west-1.compute.amazonaws.com atau cn-north-1.compute.amazonaws.com.cn. Wilayah us-east-1 tidak menggunakan nama domain ini.
- ec2.internal. Hanya Wilayah us-east-1 yang menggunakan nama domain ini.
- compute-1.internal. Hanya Wilayah us-east-1 yang menggunakan nama domain ini.
- compute-1.amazonaws.com. Hanya Wilayah us-east-1 yang menggunakan nama domain ini.

Aturan yang ditentukan otomatis berikut adalah untuk pencarian DNS terbalik untuk aturan yang dibuat oleh VPC Resolver saat Anda menyetel flag untuk VPC. `enableDnsHostnames true`

- 10.in-addr.arpa
- 16.172.in-addr.arpa melalui 31.172.in-addr.arpa

- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Aturan untuk setiap rentang CIDR untuk VPC. Misalnya, jika VPC yang memiliki rentang CIDR 10.0.0.0/23, VPC Resolver membuat aturan berikut:
 - 0.0.10.in-addr.arpa
 - 1.0.10.in-addr.arpa

Aturan yang ditentukan secara otomatis berikut, untuk domain yang berhubungan dengan localhost, juga dibuat dan terkait dengan VPC ketika Anda mengatur bendera `enableDnsHostnames` untuk VPC ke `true`:

- [illegible]

VPC Resolver membuat aturan yang ditentukan otomatis berikut dan mengaitkannya dengan VPC Anda saat Anda menghubungkan VPC dengan VPC lain melalui gateway transit atau peering VPC, dan dengan dukungan DNS diaktifkan:

- Pencarian DNS terbalik untuk rentang alamat IP VPC peer, misalnya, 0.192.in-addr.arpa

Jika Anda menambahkan blok IPv4 CIDR ke VPC, VPC Resolver menambahkan aturan yang ditentukan secara otomatis untuk rentang alamat IP baru.

- Jika VPC lain berada di wilayah lain, nama domain berikut:
 - *Region-name*.compute.internal. Wilayah us-east-1 tidak menggunakan nama domain ini.
 - *Region-name*.menghitung. *amazon-domain-name*. Wilayah us-east-1 tidak menggunakan nama domain ini.
 - ec2.internal. Hanya Wilayah us-east-1 yang menggunakan nama domain ini.
 - compute-1.amazonaws.com. Hanya Wilayah us-east-1 yang menggunakan nama domain ini.

Aturan untuk semua domain lainnya

VPC Resolver menciptakan “.” (dot) aturan yang berlaku untuk semua nama domain yang tidak ditentukan sebelumnya dalam topik ini. Aturan “.” memiliki jenis Recursive, yang berarti bahwa aturan tersebut menyebabkan VPC Resolver bertindak sebagai resolver rekursif.

Pertimbangan saat membuat titik akhir masuk dan keluar

Sebelum Anda membuat titik akhir Resolver masuk dan keluar di AWS Wilayah, pertimbangkan masalah berikut.

Topik

- [Jumlah titik akhir masuk dan keluar di setiap Wilayah](#)
- [Menggunakan VPC yang sama untuk titik akhir masuk dan keluar](#)
- [Titik akhir masuk dan zona yang di-hosting privat](#)
- [Peering VPC](#)
- [Alamat IP dalam subnet bersama](#)
- [Koneksi antara jaringan Anda dan titik akhir VPCs yang Anda buat](#)
- [Ketika berbagi aturan, Anda juga berbagi titik akhir keluar](#)
- [Memilih protokol untuk titik akhir](#)
- [Menggunakan VPC Resolver yang dikonfigurasi untuk VPCs penyewaan instans khusus](#)

Jumlah titik akhir masuk dan keluar di setiap Wilayah

Saat Anda ingin mengintegrasikan DNS untuk VPCs di AWS Wilayah dengan DNS untuk jaringan Anda, Anda biasanya memerlukan satu titik akhir masuk Resolver (untuk kueri DNS yang diteruskan ke Anda VPCs) dan satu titik akhir keluar (untuk kueri yang diteruskan dari jaringan Anda). VPCs Anda dapat membuat beberapa titik akhir masuk dan beberapa titik akhir keluar, tetapi satu titik akhir masuk atau keluar cukup untuk menangani kueri DNS untuk setiap arah masing-masing. Perhatikan hal-hal berikut:

- Untuk setiap titik akhir Resolver, Anda menentukan dua atau lebih alamat IP di Availability Zone yang berbeda. Setiap alamat IP di titik akhir dapat menangani sejumlah besar kueri DNS per detik. (Untuk jumlah maksimum kueri saat ini per detik per alamat IP di titik akhir, lihat [Kuota pada Route 53 VPC Resolver](#).) Jika Anda memerlukan VPC Resolver untuk menangani lebih banyak kueri, Anda dapat menambahkan lebih banyak alamat IP ke titik akhir yang ada alih-alih menambahkan titik akhir lain.
- Harga VPC Resolver didasarkan pada jumlah alamat IP di titik akhir Anda dan pada jumlah kueri DNS yang diproses endpoint. Setiap titik akhir mencakup minimal dua alamat IP. Untuk informasi selengkapnya tentang harga Resolver VPC, lihat Harga [Amazon](#) Route 53.

- Setiap aturan menentukan titik akhir keluar tempat kueri DNS diteruskan. Jika Anda membuat beberapa titik akhir keluar di Wilayah AWS dan ingin mengaitkan beberapa atau semua aturan Resolver dengan setiap VPC, Anda perlu membuat beberapa salinan dari aturan.

Menggunakan VPC yang sama untuk titik akhir masuk dan keluar

Anda dapat membuat titik akhir masuk dan keluar di VPC yang sama atau berbeda VPCs di Wilayah yang sama.

Untuk informasi selengkapnya, lihat [Praktik terbaik untuk Amazon Route 53](#).

Titik akhir masuk dan zona yang di-hosting privat

Jika Anda ingin VPC Resolver menyelesaikan kueri DNS masuk menggunakan catatan di zona host pribadi, kaitkan zona host pribadi dengan VPC tempat Anda membuat titik akhir masuk. Untuk informasi tentang mengaitkan zona yang dihosting pribadi dengan VPCs, lihat [Bekerja dengan zona yang di-hosting privat](#).

Peering VPC

Anda dapat menggunakan VPC apa pun di AWS Wilayah untuk titik akhir masuk atau keluar terlepas dari apakah VPC yang Anda pilih diintegrasikan dengan yang lain. VPCs Untuk informasi selengkapnya, lihat [Menyambungkan Amazon Virtual Private Cloud VPC](#).

Alamat IP dalam subnet bersama

Ketika membuat titik akhir masuk atau keluar, Anda dapat menentukan alamat IP di subnet bersama hanya jika VPC dibuat oleh akun saat ini. Jika akun lain membuat VPC dan berbagi subnet di VPC dengan akun, Anda tidak dapat menentukan alamat IP di subnet tersebut. Untuk informasi selengkapnya tentang subnet bersama, lihat [Bekerja dengan berbagi VPCs](#) di Panduan Pengguna Amazon VPC.

Koneksi antara jaringan Anda dan titik akhir VPCs yang Anda buat

Anda harus memiliki salah satu koneksi berikut antara jaringan Anda dan titik akhir VPCs yang Anda buat di:

- Titik akhir masuk – Anda harus menyiapkan koneksi [Direct Connect](#) atau [koneksi VPN](#) antara jaringan Anda dan setiap VPC tempat Anda membuat titik akhir.

- Titik akhir keluar – Anda harus menyiapkan koneksi [Direct Connect](#), [koneksi VPN](#), atau [gateway penerjemahan alamat jaringan \(NAT\)](#) antara jaringan Anda dan setiap VPC tempat Anda membuat jaringan.

Ketika berbagi aturan, Anda juga berbagi titik akhir keluar

Saat membuat aturan, Anda menentukan titik akhir keluar yang ingin digunakan VPC Resolver untuk meneruskan kueri DNS ke jaringan Anda. Jika Anda membagikan aturan dengan AWS akun lain, Anda juga secara tidak langsung membagikan titik akhir keluar yang Anda tentukan dalam aturan. Jika Anda menggunakan lebih dari satu AWS akun untuk membuat VPCs di AWS Wilayah, Anda dapat melakukan hal berikut:

- Buat satu titik akhir keluar di Wilayah.
- Buat aturan menggunakan satu AWS akun.
- Bagikan aturan dengan semua AWS akun yang dibuat VPCs di Wilayah.

Ini memungkinkan Anda menggunakan satu titik akhir keluar di Wilayah untuk meneruskan kueri DNS ke jaringan Anda dari beberapa VPCs meskipun VPCs dibuat menggunakan akun yang berbeda. AWS

Memilih protokol untuk titik akhir

Protokol endpoint menentukan bagaimana data ditransmisikan ke titik akhir masuk dan dari titik akhir keluar. Enkripsi query DNS untuk lalu lintas VPC tidak diperlukan karena setiap aliran paket pada jaringan secara individual diotorisasi terhadap aturan untuk memvalidasi sumber dan tujuan yang benar sebelum dikirim dan dikirim. Sangat tidak mungkin bagi informasi untuk secara sewenang-wenang melewati antar entitas tanpa secara khusus diberi wewenang oleh entitas pengirim dan penerima. Jika sebuah paket dialihkan ke tujuan tanpa aturan yang cocok dengannya, paket tersebut dijatuhkan. Untuk informasi selengkapnya, lihat [fitur VPC](#).

Protokol yang tersedia adalah:

- Do53: DNS melalui port 53. Data disampaikan dengan menggunakan VPC Resolver tanpa enkripsi tambahan. Meskipun data tidak dapat dibaca oleh pihak eksternal, data dapat dilihat di dalam AWS jaringan. Menggunakan UDP atau TCP untuk mengirim paket. Do53 terutama digunakan untuk lalu lintas di dalam dan di antara Amazon VPCs. Saat ini, ini adalah satu-satunya protokol yang tersedia untuk titik akhir masuk delegasi.

- DoH: Data ditransmisikan melalui sesi HTTPS terenkripsi. DoH menambahkan tingkat keamanan tambahan di mana data tidak dapat didekripsi oleh pengguna yang tidak sah, dan tidak dapat dibaca oleh siapa pun kecuali penerima yang dituju. Tidak tersedia untuk titik akhir masuk delegasi.
- DOH-FIPS: Data ditransmisikan melalui sesi HTTPS terenkripsi yang sesuai dengan standar kriptografi FIPS 140-2. Didukung hanya untuk titik akhir inbound. Untuk informasi lebih lanjut, lihat [FIPS PUB 140-2](#). Tidak tersedia untuk titik akhir masuk delegasi.

Untuk titik akhir inbound tipe Forward, Anda dapat menerapkan protokol sebagai berikut:

- Kombinasi Do53 dan DoH.
- Kombinasi Do53 dan DoH-FIPS.
- Do53 saja.
- DoH saja.
- DoH-FIPS saja.
- Tidak ada, yang diperlakukan sebagai Do53.

Untuk titik akhir keluar, Anda dapat menerapkan protokol sebagai berikut:

- Kombinasi Do53 dan DoH.
- Do53 saja.
- DoH saja.
- Tidak ada, yang diperlakukan sebagai Do53.

Lihat juga [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#) dan [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar](#).

Menggunakan VPC Resolver yang dikonfigurasi untuk VPCs penyewaan instans khusus

Ketika membuat titik akhir Resolver, Anda tidak dapat menentukan VPC dengan [atribut penghunian instans](#) yang diatur ke `dedicated`. VPC Resolver tidak berjalan pada perangkat keras penyewa tunggal.

Anda masih dapat menggunakan VPC Resolver untuk menyelesaikan kueri DNS yang berasal dari VPC. Buat setidaknya satu VPC yang memiliki atribut penhunian instans yang diatur ke default, dan tentukan VPC tersebut ketika Anda membuat titik akhir masuk dan keluar.

Ketika membuat aturan penerusan, Anda dapat mengaitkannya dengan VPC apa pun, terlepas dari pengaturan untuk atribut penghunian instans.

Ketersediaan dan penskalaan Route 53 VPC Resolver

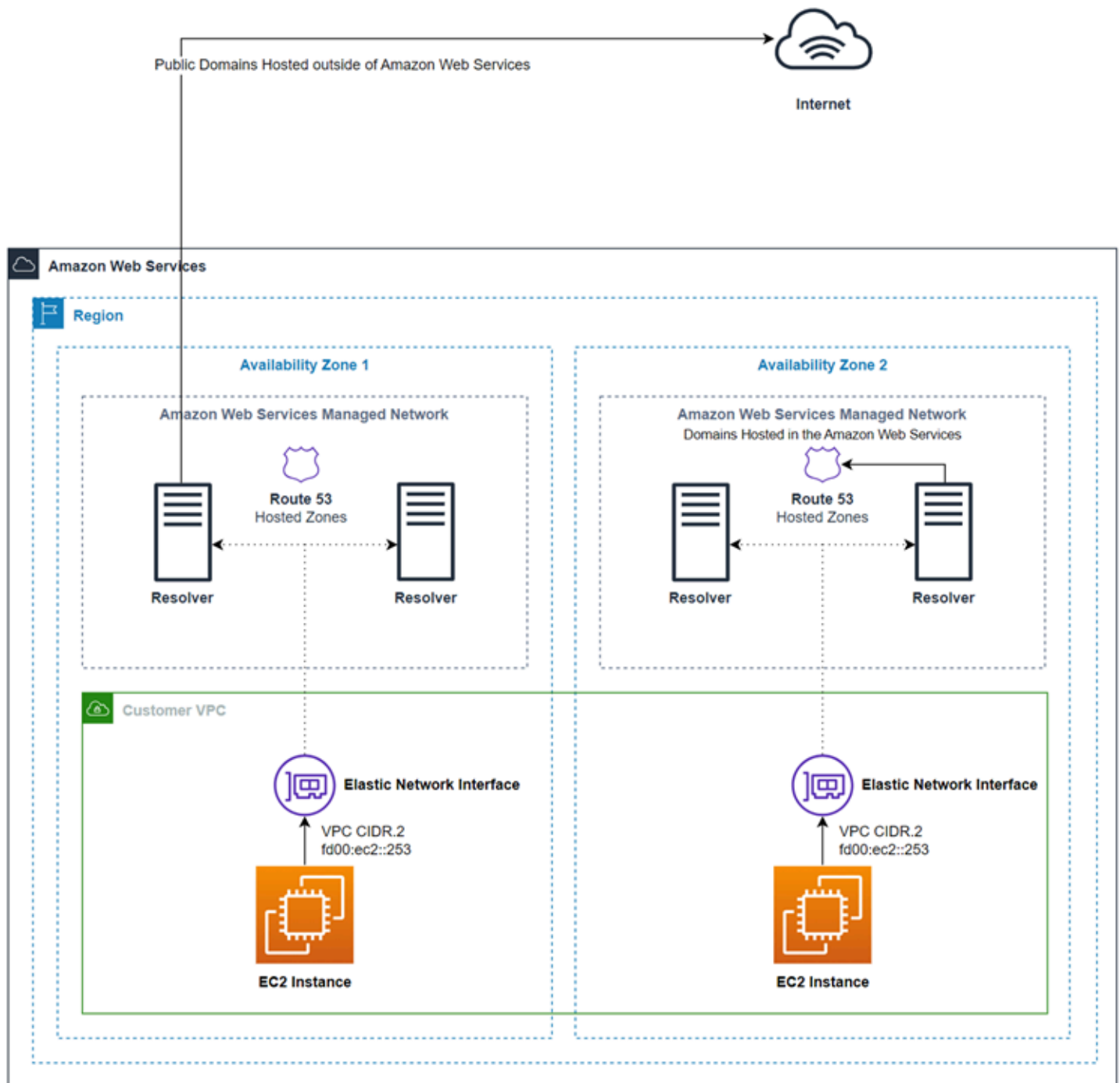
Route 53 VPC Resolver, berjalan di alamat Amazon VPC CIDR + 2 dan fd00:ec2::253, tersedia secara default di semua, dan merespons secara rekursif kueri DNS untuk catatan publik, nama DNS khusus Amazon VPC, VPCs dan zona host pribadi Route 53. Ada dua komponen yang sangat tersedia, transparan bagi pengguna, yang membentuk Route 53 VPC Resolver: layanan Nitro Resolver dan armada Zonal Resolver. Layanan Nitro Resolver adalah layanan yang berjalan di kartu Nitro pada instance Nitro dan Dom0 dalam instance generasi yang lebih tua, dan mengkonsumsi paket yang ditujukan ke Route 53 VPC Resolver secara lokal di server host. Untuk informasi selengkapnya, lihat [Desain Keamanan Sistem AWS Nitro](#).

Layanan Nitro Resolver membawa cache lokal yang dapat membantu mengurangi latensi dengan menanggapi kueri berulang yang dibuat dalam waktu singkat oleh sebuah instance. Ketika layanan Nitro Resolver menerima kueri yang tidak memiliki jawaban cache, ia meneruskan kueri ke armada Zonal Resolver, armada resolver yang sangat tersedia biasanya di Availability Zone yang sama dengan instance. Ketika ada kegagalan menangani kueri oleh server nama hulu atau komponen lain di jalur, layanan Nitro Resolver sering dapat menangani kegagalan ini secara transparan tanpa berdampak pada beban kerja yang berjalan pada instance. Selanjutnya, jika Resolver menemukan batas waktu kueri, koneksi yang ditolak, atau SERVFAILS dari server nama domain, Resolver dapat merespons dengan jawaban cache di luar nilai Time-To-Live (TTL) untuk meningkatkan ketersediaan. Pertanyaan antara layanan Nitro Resolver dan armada Zonal Resolver dibatasi pada jaringan yang dikontrol ketat di luar VPC pelanggan, yang tidak dapat diakses oleh pelanggan dan tunduk pada kontrol keamanan yang ketat. Dengan menangani pertanyaan antara layanan Nitro Resolver dan armada Zonal Resolver di luar VPC, pelanggan dicegah untuk mencegah kueri DNS di dalam VPC mereka. Kueri yang ditujukan untuk memberi nama server di luar AWS akan melintasi internet publik, yang berasal dari alamat IP publik milik armada Zonal Resolver. Kami tidak mendukung atribut EDNS0 -Client Subnet hari ini, yang berarti semua kueri yang ditujukan untuk server nama DNS publik tidak menyertakan informasi tentang alamat IP pelanggan asal.

Layanan Nitro Resolver adalah bagian dari layanan Link-Local pada instance. Layanan Link-Local meliputi Route 53 VPC Resolver, Amazon Time Service (NTP), Layanan Metadata Instans

(IMDS) dan Layanan Lisensi Windows (untuk instance Windows). Layanan ini diskalakan dengan setiap elastic network interface yang Anda buat di VPC Anda, dan setiap antarmuka jaringan memungkinkan 1024 paket per detik (PPS) yang ditujukan untuk layanan Link-Local. Paket yang melebihi batas ini ditolak. Anda dapat menentukan apakah Anda telah melampaui batas ini dari `linklocal_allowance_exceeded` nilai yang dikembalikan oleh `ethtool`. Untuk informasi selengkapnya tentang `ethtool`, lihat [Memantau performa jaringan untuk instans Amazon EC2 Anda](#) di Panduan Pengguna Amazon EC2. Metrik ini juga dapat dilaporkan ke CloudWatch metrik oleh CloudWatch Agen. Karena Resolver VPC Route 53 diimplementasikan per antarmuka jaringan, resolusi ini menskalakan dan menjadi lebih andal saat Anda menambahkan lebih banyak instance di lebih banyak Availability Zone. Tidak ada batasan agregat per VPC pada jumlah kueri, sehingga Resolver VPC Route 53 dapat menskalakan dalam batas-batas VPC, yang secara inheren didasarkan pada penggunaan alamat jaringan (NAU). Untuk informasi selengkapnya, lihat [Penggunaan Alamat Jaringan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Diagram berikut menunjukkan ikhtisar tentang bagaimana Route 53 VPC Resolver menyelesaikan kueri DNS dalam Availability Zones.



Mulai menggunakan Route 53 VPC Resolver

Konsol Resolver VPC Route 53 menyertakan wizard yang memandu Anda melalui langkah-langkah berikut untuk memulai dengan VPC Resolver:

- Membuat titik akhir: masuk, keluar, atau keduanya.

- Untuk titik akhir keluar, buat satu atau lebih aturan penerusan, yang menentukan nama domain yang kueri DNS-nya ingin Anda rutekan ke jaringan.
- Jika Anda membuat titik akhir keluar, pilih VPC yang ingin Anda kaitkan dengan aturan.

Untuk mengkonfigurasi Route 53 VPC Resolver menggunakan wizard

1. Masuk ke Konsol Manajemen AWS dan buka konsol VPC Resolver di <https://console.aws.amazon.com/route53resolver/>
2. Pada halaman Selamat Datang di Route 53 VPC Resolver, pilih Konfigurasi titik akhir.
3. Pada bilah navigasi, pilih Wilayah tempat Anda ingin membuat titik akhir Resolver.
4. Di bawah Konfigurasi dasar, pilih arah yang Anda inginkan untuk meneruskan kueri DNS:
 - Inbound dan outbound: Wizard memandu Anda melalui pengaturan yang memungkinkan Anda meneruskan kueri DNS dari resolver di jaringan Anda ke VPC Resolver di VPC, dan meneruskan kueri tertentu (seperti example.com atau example.net) dari VPC ke resolver di jaringan Anda.
 - Inbound only: Wizard memandu Anda melalui pengaturan yang memungkinkan Anda meneruskan kueri DNS dari resolver di jaringan Anda ke VPC Resolver dalam VPC.
 - Keluar saja: Wizard memandu Anda melalui pengaturan yang memungkinkan Anda meneruskan kueri yang ditentukan dari VPC ke penyelesai di jaringan.
5. Pilih Berikutnya.
6. Jika Anda memilih Masuk dan keluar atau Masuk saja, masukkan nilai yang berlaku untuk mengonfigurasi titik akhir masuk. Kemudian lanjutkan dengan langkah 7. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#).

Jika Anda memilih Keluar saja, lewati ke langkah 7.
7. Masukkan nilai yang berlaku untuk mengonfigurasi titik akhir keluar. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar](#).
8. Jika Anda memilih Masuk dan keluar atau Keluar saja, masukkan nilai yang berlaku untuk membuat aturan. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit aturan](#).
9. Pada halaman Tinjau dan buat, konfirmasi pengaturan yang Anda tentukan pada halaman sebelumnya sudah benar. Jika perlu, pilih Edit untuk bagian yang berlaku, dan perbarui pengaturan. Setelah Anda puas dengan pengaturan, pilih Kirim.

 Note

Membuat titik akhir keluar membutuhkan waktu satu atau dua menit. Anda tidak dapat membuat titik akhir keluar lain hingga yang pertama selesai dibuat.

10. Jika Anda ingin membuat lebih banyak aturan, lihat [Mengelola aturan penerusan](#).
11. Jika Anda membuat titik akhir keluar, konfigurasi penyelesai DNS di jaringan guna meneruskan kueri DNS yang ada ke alamat IP untuk titik akhir masuk. Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi DNS.

Meneruskan kueri DNS masuk ke VPCs

Untuk meneruskan kueri DNS dari jaringan Anda ke VPC Resolver, Anda membuat titik akhir masuk. Titik akhir masuk menentukan alamat IP (dari rentang alamat IP yang tersedia untuk VPC) yang Anda inginkan untuk diteruskan oleh penyelesai DNS di jaringan. Alamat IP tersebut bukan alamat IP publik, jadi untuk setiap titik akhir masuk, Anda perlu menghubungkan VPC Anda ke jaringan Anda menggunakan Direct Connect koneksi atau koneksi VPN.

Saat menerapkan delegasi masuk, Anda mendelegasikan otoritas DNS untuk subdomain dari infrastruktur DNS lokal ke VPC Resolver. Untuk mengonfigurasi delegasi ini dengan benar, Anda harus menggunakan alamat IP titik akhir masuk sebagai catatan lem (catatan NS) di server nama lokal untuk subdomain yang didelegasikan. Misalnya, jika Anda mendelegasikan subdomain “aws.example.com” ke VPC Resolver melalui titik akhir delegasi masuk dengan alamat IP 10.0.1.100 dan 10.0.1.101, Anda akan membuat catatan NS di server DNS lokal yang menunjuk “aws.example.com” ke alamat IP ini. Ini memastikan bahwa kueri DNS untuk subdomain yang didelegasikan dirutekan dengan benar ke Resolver VPC melalui titik akhir masuk, memungkinkan Resolver VPC merespons dengan catatan dari zona host pribadi terkait.

Mengonfigurasi penerusan masuk

Untuk membuat titik akhir masuk, lakukan prosedur berikut.

Cara membuat titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir masuk.

3. Pada bilah navigasi, pilih Wilayah tempat Anda ingin membuat titik akhir masuk.
4. Pilih Buat titik akhir masuk.
5. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#).
6. Pilih Buat.
7. Mengonfigurasi penyelesai DNS di jaringan guna meneruskan kueri DNS yang ada ke alamat IP untuk titik akhir masuk. Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi DNS.

Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk

Saat Anda membuat atau mengedit titik akhir masuk, tentukan nilai berikut:

ID Outpost

Jika Anda membuat titik akhir untuk Resolver VPC di VPC, AWS Outposts ini adalah ID. AWS Outposts

Nama titik akhir

Nama ramah yang memudahkan Anda menemukan titik akhir masuk di dasbor.

Kategori titik akhir

Pilih Default atau Delegasi. Jika kategorinya Default, resolver di jaringan Anda meneruskan permintaan DNS ke alamat IP titik akhir masuk. Ketika kategorinya adalah Delegasi, otoritas untuk domain didelegasikan ke Resolver VPC.

VPC dalam Wilayah region-name

Semua kueri DNS masuk dari jaringan Anda melewati VPC ini dalam perjalanan ke VPC Resolver.

Grup keamanan untuk titik akhir ini

ID salah satu atau beberapa grup keamanan yang ingin Anda gunakan untuk mengendalikan akses ke VPC ini. Grup keamanan yang Anda tentukan harus menyertakan satu atau lebih aturan masuk. Aturan masuk harus mengizinkan akses TCP dan UDP di port 53. Jika Anda menggunakan protokol DoH, Anda juga harus mengizinkan port 443 di grup keamanan. Anda tidak dapat mengubah nilai ini setelah Anda membuat titik akhir.

Beberapa aturan grup keamanan akan menyebabkan koneksi Anda dilacak dan kueri maksimum keseluruhan per detik per alamat IP untuk titik akhir masuk bisa serendah 1500. Untuk

menghindari pelacakan koneksi yang disebabkan oleh grup keamanan, lihat Koneksi [yang tidak dilacak](#).

 Note

Untuk menambahkan beberapa grup keamanan, gunakan AWS CLI perintah `create-resolver-endpoint`. Untuk informasi selengkapnya, lihat [create-resolver-endpoint](#)

Untuk informasi selengkapnya, lihat [Grup keamanan untuk VPC Anda](#) di Panduan pengguna Amazon VPC.

Tipe titik akhir

Jenis endpoint dapat berupa IPv4, IPv6, atau alamat IP dual-stack. Untuk titik akhir dual-stack, titik akhir akan memiliki keduanya IPv4 dan IPv6 alamat yang dapat diteruskan oleh resolver DNS Anda di jaringan Anda.

 Note

Untuk alasan keamanan, kami menolak akses IPv6 lalu lintas langsung dari internet publik untuk semua alamat dual-stack dan IPv6 IP.

Alamat IP

Alamat IP tujuan penerusan kueri DNS yang dilakukan oleh penyelesai DNS di jaringan. Kami mengharuskan Anda untuk menentukan minimal dua alamat IP untuk redundansi. Jika Anda membuat titik akhir masuk delegasi, gunakan alamat IP ini sebagai catatan NS untuk subdomain yang ingin Anda delegasikan wewenangannya ke VPC Resolver. Perhatikan hal-hal berikut:

Beberapa Availability Zone

Kami menyarankan Anda menentukan alamat IP di setidaknya dua Availability Zone. Secara opsional Anda dapat menentukan alamat IP tambahan di Availability Zone tersebut atau lainnya.

Alamat IP dan antarmuka jaringan elastis Amazon VPC

Untuk setiap kombinasi Availability Zone, Subnet, dan alamat IP yang Anda tentukan, VPC Resolver membuat antarmuka elastis network Amazon VPC. Untuk jumlah maksimum kueri

DNS saat ini per detik per alamat IP di titik akhir, lihat [Kuota pada Route 53 VPC Resolver](#). Untuk informasi tentang harga untuk setiap elastic network interface, lihat “Amazon Route 53” di halaman [harga Amazon Route 53](#).

 Note

Titik akhir Resolver memiliki alamat IP pribadi. Alamat IP ini tidak akan berubah selama masa hidup titik akhir.

Untuk setiap alamat IP, tentukan nilai berikut. Setiap alamat IP harus berada dalam Availability Zone di VPC yang Anda tentukan di VPC dalam Wilayah region-name.

Zona Ketersediaan

Availability Zone yang akan dilewati kueri DNS dalam perjalanan ke VPC Anda. Availability Zone yang Anda tentukan harus dikonfigurasi dengan subnet.

Subnet

Subnet yang berisi alamat IP yang ingin Anda tetapkan ke titik akhir Resolver Anda. ENIs Ini adalah alamat yang akan Anda kirim kueri DNS. Subnet harus memiliki alamat IP yang tersedia.

Alamat IP subnet harus sesuai dengan tipe Endpoint.

Alamat IP

Alamat IP yang ingin Anda tetapkan ke titik akhir masuk.

Pilih apakah Anda ingin VPC Resolver memilih alamat IP untuk Anda dari antara alamat IP yang tersedia di subnet yang ditentukan, atau Anda ingin menentukan alamat IP sendiri.

Jika Anda memilih untuk menentukan alamat IP sendiri, masukkan salah satu IPv4 atau IPv6 alamat, atau keduanya.

Protokol

Protokol endpoint menentukan bagaimana data ditransmisikan ke titik akhir inbound. Pilih satu atau beberapa protokol sesuai tingkat keamanan yang dibutuhkan.

- Do53: (Default) Data diteruskan menggunakan Route 53 VPC Resolver tanpa enkripsi tambahan. Meskipun data tidak dapat dibaca oleh pihak eksternal, data dapat dilihat di dalam

AWS jaringan. Ini adalah satu-satunya protokol yang saat ini tersedia untuk kategori titik akhir masuk Delegasi.

- DoH: Data ditransmisikan melalui sesi HTTPS terenkripsi. DoH menambahkan tingkat keamanan tambahan di mana data tidak dapat didekripsi oleh pengguna yang tidak sah, dan tidak dapat dibaca oleh siapa pun kecuali penerima yang dituju.
- DOH-FIPS: Data ditransmisikan melalui sesi HTTPS terenkripsi yang sesuai dengan standar kriptografi FIPS 140-2. Didukung hanya untuk titik akhir inbound. Untuk informasi lebih lanjut, lihat [FIPS PUB 140-2](#).

 Note

Untuk titik akhir masuk DOH/DOH-FIPS, ada masalah yang diketahui dengan IP sumber yang salah yang diterbitkan dalam pencatatan kueri VPC Resolver.

Untuk titik akhir masuk, Anda dapat menerapkan protokol sebagai berikut:

- Kombinasi Do53 dan DoH.
- Kombinasi Do53 dan DoH-FIPS.
- Do53 saja.
- DoH saja.
- DoH-FIPS saja.
- Tidak ada, yang diperlakukan sebagai Do53.

 Important

Anda tidak dapat mengubah protokol titik akhir masuk secara langsung dari hanya Do53 menjadi hanya DoH, atau DOH-FIP. Ini untuk mencegah gangguan mendadak pada lalu lintas masuk yang bergantung pada Do53. Untuk mengubah protokol dari Do53 ke DoH, atau DoH-FIP, Anda harus terlebih dahulu mengaktifkan Do53 dan DoH, atau Do53 dan DoH-FIP, untuk memastikan bahwa semua lalu lintas yang masuk telah ditransfer menggunakan protokol DoH, atau DoH-FIP, dan kemudian menghapus Do53.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Mengelola titik akhir masuk

Untuk mengelola titik akhir masuk, lakukan prosedur yang berlaku.

Topik

- [Melihat dan mengedit titik akhir masuk](#)
- [Melihat status titik akhir masuk](#)
- [Menghapus titik akhir masuk](#)

Melihat dan mengedit titik akhir masuk

Untuk melihat dan mengedit pengaturan titik akhir masuk, lakukan prosedur berikut.

Cara melihat dan mengedit pengaturan untuk titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir masuk.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir masuk.
4. Pilih opsi untuk titik akhir yang pengaturannya ingin Anda lihat atau edit.
5. Pilih Tampilkan detail atau Edit.

Untuk informasi tentang nilai titik akhir masuk, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#).

6. Jika Anda memilih Edit, masukkan nilai yang berlaku, dan pilih Simpan.

Melihat status titik akhir masuk

Untuk melihat status titik akhir masuk, lakukan prosedur berikut.

Cara melihat status titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir masuk.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir masuk. Kolom Status berisi salah satu nilai berikut:

Membuat

VPC Resolver membuat dan mengonfigurasi satu atau lebih antarmuka jaringan VPC Amazon untuk titik akhir ini.

Operasional

Antarmuka jaringan VPC Amazon untuk titik akhir ini dikonfigurasi dengan benar dan dapat meneruskan kueri DNS masuk atau keluar antara jaringan Anda dan VPC Resolver.

Memperbarui

VPC Resolver mengaitkan atau memisahkan satu atau lebih antarmuka jaringan dengan titik akhir ini.

Memulihkan otomatis

VPC Resolver mencoba memulihkan satu atau lebih antarmuka jaringan yang terkait dengan titik akhir ini. Selama proses pemulihan, titik akhir berfungsi dengan kapasitas terbatas karena batas jumlah kueri DNS per alamat IP (per antarmuka jaringan). Untuk batas saat ini, lihat [Kuota pada Route 53 VPC Resolver](#).

Diperlukan tindakan

Titik akhir ini tidak sehat, dan VPC Resolver tidak dapat memulihkannya secara otomatis. Untuk mengatasi masalah, kami sarankan Anda memeriksa setiap alamat IP yang dikaitkan dengan titik akhir. Untuk setiap alamat IP yang tidak tersedia, tambahkan alamat IP lain, lalu hapus alamat IP yang tidak tersedia. (Titik akhir harus selalu menyertakan setidaknya dua alamat IP.) Status Diperlukan tindakan dapat memiliki berbagai penyebab. Berikut adalah dua penyebab umum:

- Satu atau lebih antarmuka jaringan yang terkait dengan titik akhir dihapus menggunakan Amazon VPC.
- Antarmuka jaringan tidak dapat dibuat karena beberapa alasan yang berada di luar kendali VPC Resolver.

Menghapus

VPC Resolver menghapus titik akhir ini dan antarmuka jaringan terkait.

Menghapus titik akhir masuk

Untuk menghapus titik akhir masuk, lakukan prosedur berikut.

Important

Jika Anda menghapus titik akhir masuk, kueri DNS dari jaringan Anda tidak lagi diteruskan ke VPC Resolver di VPC yang Anda tentukan di titik akhir.

Cara menghapus titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir masuk.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir masuk.
4. Pilih opsi untuk titik akhir yang ingin Anda hapus.
5. Pilih Hapus.
6. Untuk mengonfirmasi bahwa Anda ingin menghapus titik akhir, masukkan nama titik akhir dan pilih Kirim.

Meneruskan kueri DNS keluar ke jaringan Anda

Untuk meneruskan kueri DNS yang berasal dari instans Amazon EC2 di satu atau beberapa VPCs ke jaringan Anda, Anda membuat titik akhir keluar dan satu atau beberapa aturan:

Titik akhir keluar

Untuk meneruskan kueri DNS dari jaringan Anda VPCs ke jaringan Anda, Anda membuat titik akhir keluar. Titik akhir keluar menentukan alamat IP tempat kueri berasal. Alamat IP tersebut, yang Anda pilih dari kisaran alamat IP yang tersedia untuk VPC, bukanlah alamat IP publik. Ini berarti bahwa, untuk setiap titik akhir keluar, Anda perlu menghubungkan VPC ke jaringan menggunakan koneksi Direct Connect, koneksi VPN, atau gateway penerjemahan alamat jaringan (NAT). Perhatikan bahwa Anda dapat menggunakan titik akhir keluar yang sama untuk beberapa VPCs di Wilayah yang sama, atau Anda dapat membuat beberapa titik akhir keluar. Jika ingin titik akhir keluar digunakan DNS64, Anda dapat mengaktifkan DNS64 menggunakan

Amazon Virtual Private Cloud. Untuk informasi selengkapnya, lihat [DNS64 dan NAT64](#) di Panduan Pengguna Amazon VPC.

IP target dari aturan Resolver VPC dipilih secara acak oleh VPC Resolver dan tidak ada preferensi untuk memilih IP target tertentu di atas yang lain. Jika IP target tidak menanggapi permintaan DNS yang diteruskan, Resolver VPC akan mencoba lagi ke alamat IP acak di antara target. IPs

Pastikan bahwa semua alamat IP target dapat dijangkau dari titik akhir Resolver. Jika VPC Resolver tidak dapat meneruskan kueri DNS keluar ke salah satu IP target, itu dapat menyebabkan waktu resolusi DNS diperpanjang.

Aturan

Untuk menentukan nama domain kueri yang ingin diteruskan ke penyelesai DNS di jaringan Anda, buatlah satu atau lebih aturan. Setiap aturan penerusan menentukan satu nama domain. Anda kemudian mengaitkan aturan dengan VPCs yang ingin Anda teruskan kueri ke jaringan Anda.

Aturan delegasi keluar mengikuti prinsip delegasi tertentu yang berbeda dari aturan penerusan standar. Saat Anda membuat aturan delegasi, VPC Resolver mengevaluasi catatan delegasi dalam aturan terhadap catatan NS dalam respons DNS untuk menentukan apakah delegasi harus terjadi. Resolver VPC akan mendelegasikan otoritas ke resolver lokal Anda hanya jika ada kecocokan antara konfigurasi aturan delegasi dan catatan NS aktual yang ditampilkan dalam respons DNS. Tidak seperti aturan penerusan yang mengarahkan kueri berdasarkan pencocokan nama domain, aturan delegasi menghormati rantai delegasi DNS dan hanya diaktifkan ketika server nama otoritatif dalam respons cocok dengan konfigurasi delegasi.

Untuk informasi selengkapnya, lihat topik berikut:

- [Private hosted zones that have overlapping namespaces](#)
- [Private hosted zones and Route 53 VPC Resolver rules](#)

Mengonfigurasi penerusan keluar

Untuk mengonfigurasi Resolver VPC untuk meneruskan kueri DNS yang berasal dari VPC Anda ke jaringan Anda, lakukan prosedur berikut.

 Important

Setelah Anda membuat titik akhir keluar, Anda harus membuat satu atau beberapa aturan dan mengaitkannya dengan satu atau lebih VPCs Untuk menentukan nama domain kueri DNS yang ingin diteruskan ke jaringan Anda.

Cara membuat titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir keluar.
3. Pada bilah navigasi, pilih Wilayah tempat Anda ingin membuat titik akhir keluar.
4. Pilih Buat titik akhir keluar.
5. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar](#).
6. Pilih Buat.

 Note

Membuat titik akhir keluar membutuhkan waktu satu atau dua menit. Anda tidak dapat membuat titik akhir keluar lain hingga yang pertama selesai dibuat.

7. Membuat satu atau lebih aturan untuk menentukan nama domain kueri DNS yang ingin diteruskan ke jaringan Anda. Untuk informasi selengkapnya, lihat prosedur berikutnya.

Untuk membuat satu atau lebih aturan penerusan, lakukan prosedur berikut.

Untuk membuat aturan penerusan dan mengaitkan aturan dengan satu atau lebih VPCs

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda ingin membuat aturan.
4. Pilih Buat aturan.

5. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit aturan](#).
6. Pilih Simpan.
7. Untuk menambahkan aturan lain, ulangi langkah 4 hingga 6.

Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar

Saat Anda membuat atau mengedit titik akhir keluar, tentukan nilai berikut:

ID Outpost

Jika Anda membuat titik akhir untuk Resolver VPC di VPC, AWS Outposts ini adalah ID. AWS Outposts

Nama titik akhir

Nama ramah yang memudahkan Anda menemukan titik akhir keluar di dasbor.

VPC dalam Wilayah region-name

Semua kueri DNS keluar akan mengalir melalui VPC ini dalam perjalanan ke jaringan Anda.

Grup keamanan untuk titik akhir ini

ID salah satu atau beberapa grup keamanan yang ingin Anda gunakan untuk mengendalikan akses ke VPC ini. Grup keamanan yang Anda tentukan harus menyertakan satu atau lebih aturan keluar. Aturan keluar harus mengizinkan akses TCP dan UDP di port yang Anda gunakan untuk kueri DNS di jaringan. Anda tidak dapat mengubah nilai ini setelah membuat titik akhir.

Beberapa aturan grup keamanan akan menyebabkan koneksi Anda dilacak dan berpotensi memengaruhi kueri maksimum per detik dari titik akhir keluar ke server nama target Anda. Untuk menghindari pelacakan koneksi yang disebabkan oleh grup keamanan, lihat Koneksi [yang tidak dilacak](#).

Untuk informasi selengkapnya, lihat [Grup keamanan untuk VPC Anda](#) di Panduan pengguna Amazon VPC.

Tipe titik akhir

Jenis endpoint dapat berupa IPv4, IPv6, atau alamat IP dual-stack. Untuk titik akhir dual-stack, titik akhir akan memiliki keduanya IPv4 dan IPv6 alamat yang dapat diteruskan oleh resolver DNS Anda di jaringan Anda.

 Note

Untuk alasan keamanan, kami menolak akses IPv6 lalu lintas langsung ke internet publik untuk semua alamat dual-stack dan IPv6 IP.

Alamat IP

Alamat IP di VPC Anda yang Anda inginkan VPC Resolver untuk meneruskan kueri DNS dalam perjalanan ke resolver di jaringan Anda. Ini bukan alamat IP dari resolver DNS di jaringan Anda; Anda menentukan alamat IP resolver saat Anda membuat aturan yang Anda kaitkan dengan satu atau lebih VPCs Kami mengharuskan Anda untuk menentukan minimal dua alamat IP untuk redundansi.

 Note

Titik akhir Resolver memiliki alamat IP pribadi. Alamat IP ini tidak akan berubah selama masa hidup titik akhir.

Perhatikan hal-hal berikut:

Beberapa Availability Zone

Kami menyarankan Anda menentukan alamat IP di setidaknya dua Availability Zone. Secara opsional Anda dapat menentukan alamat IP tambahan di Availability Zone tersebut atau lainnya.

Alamat IP dan antarmuka jaringan elastis Amazon VPC

Untuk setiap kombinasi Availability Zone, Subnet, dan alamat IP yang Anda tentukan, VPC Resolver membuat antarmuka elastis network Amazon VPC. Untuk jumlah maksimum kueri DNS saat ini per detik per alamat IP di titik akhir, lihat [Kuota pada Route 53 VPC Resolver](#). Untuk informasi tentang harga untuk setiap elastic network interface, lihat “Amazon Route 53” di halaman [harga Amazon Route 53](#).

Urutan alamat IP

Anda dapat menentukan alamat IP dalam urutan apa pun. Saat meneruskan kueri DNS, VPC Resolver tidak memilih alamat IP berdasarkan urutan alamat IP yang tercantum.

Untuk setiap alamat IP, tentukan nilai berikut. Setiap alamat IP harus berada dalam Availability Zone di VPC yang Anda tentukan di VPC dalam Wilayah region-name.

Zona Ketersediaan

Availability Zone yang akan dilewati kueri DNS dalam perjalanan ke jaringan Anda. Availability Zone yang Anda tentukan harus dikonfigurasi dengan subnet.

Subnet

Subnet yang berisi alamat IP tempat kueri DNS berasal dari dalam perjalanan ke jaringan Anda. Subnet harus memiliki alamat IP yang tersedia.

Alamat IP subnet harus sesuai dengan tipe Endpoint.

Alamat IP

Alamat IP tempat kueri DNS berasal dari dalam perjalanan ke jaringan Anda.

Pilih apakah Anda ingin VPC Resolver memilih alamat IP untuk Anda dari antara alamat IP yang tersedia di subnet yang ditentukan, atau Anda ingin menentukan alamat IP sendiri.

Jika Anda memilih untuk menentukan alamat IP sendiri, masukkan IPv6 alamat IPv4 atau, atau keduanya.

Protokol

Protokol titik akhir menentukan bagaimana data ditransmisikan dari titik akhir keluar. Pilih satu atau beberapa protokol sesuai tingkat keamanan yang dibutuhkan.

- Do53: (Default) Data diteruskan menggunakan Route 53 VPC Resolver tanpa enkripsi tambahan. Meskipun data tidak dapat dibaca oleh pihak eksternal, data dapat dilihat di dalam AWS jaringan.
- DoH: Data ditransmisikan melalui sesi HTTPS terenkripsi. DoH menambahkan tingkat keamanan tambahan di mana data tidak dapat didekripsi oleh pengguna yang tidak sah, dan tidak dapat dibaca oleh siapa pun kecuali penerima yang dituju.

Untuk titik akhir keluar, Anda dapat menerapkan protokol sebagai berikut:

- Kombinasi Do53 dan DoH.
- Do53 saja.
- DoH saja.
- Tidak ada, yang diperlakukan sebagai Do53.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Nilai yang Anda tentukan ketika membuat atau mengedit aturan

Saat Anda membuat atau mengedit aturan penerusan, tentukan nilai berikut:

Nama aturan

Nama ramah yang memudahkan Anda menemukan aturan di dasbor.

Jenis aturan

Pilih nilai yang sesuai:

- Teruskan – Pilih opsi ini ketika Anda ingin meneruskan kueri DNS untuk nama domain tertentu ke penyelesai di jaringan.
- Delegasi — Pilih opsi ini ketika Anda ingin mendelegasikan otoritas untuk subdomain, yang dihosting di zona host pribadi, ke resolver lokal Anda (atau ke Resolver VPC di VPC lain).
- Sistem — Pilih opsi ini jika Anda ingin VPC Resolver secara selektif mengganti perilaku yang ditentukan dalam aturan penerusan. Saat Anda membuat aturan sistem, VPC Resolver menyelesaikan kueri DNS untuk subdomain tertentu yang akan diselesaikan oleh penyelesai DNS di jaringan Anda.

Secara default, aturan penerusan berlaku untuk nama domain dan semua subdomainnya. Jika Anda ingin meneruskan kueri untuk domain ke penyelesai di jaringan tetapi Anda tidak ingin meneruskan kueri untuk beberapa subdomain, buatlah aturan sistem untuk subdomain. Misalnya, jika Anda membuat aturan penerusan untuk `example.com` tetapi tidak ingin meneruskan kueri untuk `acme.example.com`, buatlah aturan sistem dan tentukan `acme.example.com` untuk nama domain.

Catatan delegasi — hanya untuk aturan delegasi

Kueri DNS yang mach ke domain ini diteruskan ke resolver di jaringan Anda.

Note

Sebagai prasyarat untuk aturan delegasi, Anda harus membuat catatan NS di zona host pribadi, saat menggunakan zona host pribadi untuk delegasi keluar. Catatannya adalah:

NS - Server nama untuk didelegasikan melalui titik akhir keluar Resolver dengan aturan delegasi. Untuk informasi selengkapnya, lihat [Tipe catatan NS](#).

VPCs yang menggunakan aturan ini

VPCs Yang menggunakan aturan ini untuk meneruskan kueri DNS untuk nama domain tertentu atau nama. Anda dapat menerapkan aturan untuk VPCs sebanyak yang Anda inginkan.

Nama domain — hanya untuk aturan penerusan

Kueri DNS untuk nama domain ini diteruskan ke alamat IP yang ditentukan dalam Alamat IP target. Misalnya, Anda dapat menentukan domain tertentu (example.com), domain tingkat atas (com), atau titik (.) untuk meneruskan semua kueri DNS. Untuk informasi selengkapnya, lihat [Bagaimana VPC Resolver menentukan apakah nama domain dalam kueri cocok dengan aturan apa pun](#).

Titik akhir keluar

VPC Resolver meneruskan kueri DNS melalui titik akhir keluar yang Anda tentukan di sini ke alamat IP yang Anda tentukan di alamat IP Target.

Alamat IP target

Jika kueri DNS cocok dengan nama domain yang Anda tentukan dalam Nama domain, titik akhir keluar meneruskan kueri ke alamat IP yang Anda tentukan di sini. Biasanya, ini adalah alamat IP penyelesai DNS pada jaringan Anda.

Alamat IP target tersedia hanya ketika nilai Jenis aturan adalah Teruskan.

Tentukan IPv4 atau IPv6 alamat, protokol, dan yang ingin ServerNameIndication Anda gunakan untuk titik akhir. ServerNameIndication hanya berlaku jika protokol yang dipilih adalah DoH.

Menyelesaikan alamat IP target FQDN dari resolver DoH di jaringan Anda melalui titik akhir keluar tidak didukung. Titik akhir keluar memerlukan alamat IP target resolver DoH di jaringan Anda untuk meneruskan kueri DoH ke. Jika resolver DoH di jaringan Anda membutuhkan FQDN di TLS SNI dan di header Host HTTP, harus disediakan. ServerNameIndication

ServerNameIndication

Indikasi Nama Server server DoH yang ingin Anda teruskan kueri. Ini hanya digunakan jika Protokol adalah DoH.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Ini adalah tag yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Menggunakan tanda alokasi biaya](#) dalam Panduan Pengguna AWS Billing .

Mengelola titik akhir keluar

Untuk mengelola titik akhir keluar, lakukan prosedur yang berlaku.

Topik

- [Melihat dan mengedit titik akhir keluar](#)
- [Melihat status titik akhir keluar](#)
- [Menghapus titik akhir keluar](#)

Melihat dan mengedit titik akhir keluar

Untuk melihat dan mengedit pengaturan titik akhir keluar, lakukan prosedur berikut.

Cara melihat dan mengedit pengaturan untuk titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir keluar.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir keluar.
4. Pilih opsi untuk titik akhir yang pengaturannya ingin Anda lihat atau edit.
5. Pilih Tampilkan detail atau Edit.

Untuk informasi tentang nilai titik akhir keluar, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar](#).

6. Jika Anda memilih Edit, masukkan nilai yang berlaku, lalu pilih Simpan.

Melihat status titik akhir keluar

Untuk melihat status titik akhir keluar, lakukan prosedur berikut.

Cara melihat status titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir keluar.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir keluar. Kolom Status berisi salah satu nilai berikut:

Membuat

VPC Resolver membuat dan mengonfigurasi satu atau lebih antarmuka jaringan VPC Amazon untuk titik akhir ini.

Operasional

Antarmuka jaringan VPC Amazon untuk titik akhir ini dikonfigurasi dengan benar dan dapat meneruskan kueri DNS masuk atau keluar antara jaringan Anda dan VPC Resolver.

Memperbarui

VPC Resolver mengaitkan atau memisahkan satu atau lebih antarmuka jaringan dengan titik akhir ini.

Memulihkan otomatis

VPC Resolver mencoba memulihkan satu atau lebih antarmuka jaringan yang terkait dengan titik akhir ini. Selama proses pemulihan, titik akhir berfungsi dengan kapasitas terbatas karena batas jumlah kueri DNS per alamat IP (per antarmuka jaringan). Untuk batas saat ini, lihat [Kuota pada Route 53 VPC Resolver](#).

Diperlukan tindakan

Titik akhir ini tidak sehat, dan VPC Resolver tidak dapat memulihkannya secara otomatis. Untuk mengatasi masalah, kami sarankan Anda memeriksa setiap alamat IP yang dikaitkan dengan titik akhir. Untuk setiap alamat IP yang tidak tersedia, tambahkan alamat IP lain, lalu hapus alamat IP yang tidak tersedia. (Titik akhir harus selalu menyertakan setidaknya dua alamat IP.) Status Diperlukan tindakan dapat memiliki berbagai penyebab. Berikut adalah dua penyebab umum:

- Satu atau lebih antarmuka jaringan yang terkait dengan titik akhir dihapus menggunakan Amazon VPC.
- Antarmuka jaringan tidak dapat dibuat karena beberapa alasan yang berada di luar kendali VPC Resolver.

Menghapus

VPC Resolver menghapus titik akhir ini dan antarmuka jaringan terkait.

Menghapus titik akhir keluar

Sebelum Anda dapat menghapus titik akhir, Anda harus terlebih dahulu menghapus aturan apa pun yang terkait dengan VPC.

Untuk menghapus titik akhir keluar, lakukan prosedur berikut.

Important

Jika Anda menghapus titik akhir keluar, VPC Resolver berhenti meneruskan kueri DNS dari VPC ke jaringan Anda untuk aturan yang menentukan titik akhir keluar yang dihapus.

Cara menghapus titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Titik akhir keluar.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir keluar.
4. Pilih opsi untuk titik akhir yang ingin Anda hapus.
5. Pilih Hapus.
6. Untuk mengonfirmasi bahwa Anda ingin menghapus titik akhir, masukkan nama titik akhir, lalu pilih Kirim.

Mengelola aturan penerusan

Jika Anda ingin VPC Resolver meneruskan kueri untuk nama domain tertentu ke jaringan Anda, Anda membuat satu aturan penerusan untuk setiap nama domain dan menentukan nama domain yang ingin Anda teruskan kueri.

Topik

- [Melihat dan mengedit aturan penerusan](#)
- [Membuat aturan penerusan](#)
- [Menambahkan aturan untuk pencarian terbalik](#)
- [Mengaitkan aturan penerusan dengan VPC](#)
- [Memisahkan aturan penerusan dari VPC](#)
- [Berbagi aturan Resolver dengan AWS akun lain dan menggunakan aturan bersama](#)
- [Menghapus aturan penerusan](#)
- [Aturan penerusan untuk kueri DNS terbalik di VPC Resolver](#)

Melihat dan mengedit aturan penerusan

Untuk melihat dan mengedit aturan penerusan, lakukan prosedur berikut.

Cara melihat dan mengedit pengaturan untuk aturan penerusan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat aturan.
4. Pilih opsi untuk aturan yang pengaturannya ingin Anda lihat atau edit.
5. Pilih Tampilkan detail atau Edit.

Untuk informasi tentang nilai aturan penerusan, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit aturan](#).

6. Jika Anda memilih Edit, masukkan nilai yang berlaku, lalu pilih Simpan.

Membuat aturan penerusan

Untuk membuat satu atau lebih aturan penerusan, lakukan prosedur berikut.

Untuk membuat aturan penerusan dan mengaitkan aturan dengan satu atau lebih VPCs

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda ingin membuat aturan.
4. Pilih Buat aturan.
5. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit aturan](#).
6. Pilih Simpan.
7. Untuk menambahkan aturan lain, ulangi langkah 4 hingga 6.

Menambahkan aturan untuk pencarian terbalik

Jika perlu mengontrol pencarian terbalik di VPC, Anda dapat menambahkan aturan ke titik akhir keluar penyelesaian.

Cara membuat aturan pencarian terbalik

1. Ikuti langkah-langkah dalam prosedur sebelumnya, hingga langkah 5.
2. Saat Anda menentukan aturan, masukkan catatan PTR untuk alamat IP yang Anda inginkan untuk aturan penerusan pencarian terbalik.

Misalnya, jika Anda perlu meneruskan pencarian untuk alamat di kisaran 10.0.0.0/23, masukkan dua aturan:

- 0.0.10.in-addr.arpa
- 1.0.10.in-addr.arpa

Setiap alamat IP dalam subnet tersebut akan direferensikan sebagai subdomain dari catatan PTR tersebut—misalnya, 10.0.1.161 akan memiliki alamat pencarian terbalik 161.1.0.10.in-addr.arpa, yang merupakan subdomain dari 1.0.10.in-addr.arpa.

3. Tentukan server untuk meneruskan pencarian ini.
4. Tambahkan aturan ini ke titik akhir penyelesai keluar Anda.

Perhatikan bahwa menyalakan `enableDNSHostNames` untuk VPC Anda secara otomatis akan menambahkan catatan PTR. Lihat [Apa itu Route 53 VPC Resolver?](#). Prosedur sebelumnya diperlukan hanya jika Anda ingin secara eksplisit menentukan penyelesai bagi kisaran IP yang diberikan—misalnya, ketika meneruskan kueri ke server Direktori Aktif.

Mengaitkan aturan penerusan dengan VPC

Setelah Anda membuat aturan penerusan, Anda harus mengaitkan aturan dengan satu atau lebih VPCs. Aturan hanya akan berfungsi setelah dikaitkan dengan VPC. Saat Anda mengaitkan aturan dengan VPC, Resolver VPC mulai meneruskan kueri DNS untuk nama domain yang ditentukan dalam aturan ke resolver DNS yang Anda tentukan dalam aturan. Kueri melewati titik akhir keluar yang Anda tentukan saat membuat aturan.

Untuk mengaitkan aturan penerusan dengan satu atau lebih VPCs

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat aturan.
4. Pilih nama aturan yang ingin Anda kaitkan dengan satu atau lebih VPCs.
5. Pilih Kaitkan VPC.
6. Di bawah VPCs itu gunakan aturan ini, pilih aturan VPCs yang ingin Anda kaitkan dengan aturan tersebut.
7. Pilih Tambahkan.

Memisahkan aturan penerusan dari VPC

Anda memisahkan aturan penerusan dari VPC dalam keadaan berikut:

- Untuk kueri DNS yang berasal dari VPC ini, Anda ingin VPC Resolver menghentikan penerusan kueri untuk nama domain yang ditentukan dalam aturan ke jaringan Anda.
- Anda ingin menghapus aturan penerusan. Jika aturan saat ini dikaitkan dengan satu atau lebih VPCs, Anda harus memisahkan aturan dari semua VPCs sebelum Anda dapat menghapusnya.

Jika Anda ingin memisahkan aturan penerusan dari satu atau lebih VPCs, lakukan prosedur berikut.

Cara memisahkan aturan penerusan dari VPC

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat aturan.
4. Pilih nama aturan yang ingin Anda pisahkan dari satu atau lebih VPCs.
5. Pilih opsi untuk VPC yang ingin Anda pisahkan dari aturan.
6. Pilih Pisahkan.
7. Ketik disassociate untuk mengonfirmasi.
8. Pilih Kirim.

Berbagi aturan Resolver dengan AWS akun lain dan menggunakan aturan bersama

Anda dapat membagikan aturan Resolver yang Anda buat menggunakan satu AWS akun dengan akun lain AWS. Untuk berbagi aturan, konsol Resolver VPC Route 53 terintegrasi dengan Resource Access Manager. AWS Untuk informasi lebih lanjut tentang Resource Access Manager, lihat [Panduan Pengguna Resource Access Manager](#).

Perhatikan hal-hal berikut:

Mengaitkan aturan bersama dengan VPCs

Jika AWS akun lain telah membagikan satu atau beberapa aturan dengan akun Anda, Anda dapat mengaitkan aturan dengan cara yang sama seperti Anda mengaitkan aturan yang Anda buat dengan akun Anda VPCs. VPCs Untuk informasi selengkapnya, lihat [Mengaitkan aturan penerusan dengan VPC](#).

Menghapus atau membatalkan berbagi aturan

Jika Anda berbagi aturan dengan akun lain dan kemudian menghapus aturan atau berhenti membagikannya, dan jika aturan dikaitkan dengan satu atau lebih VPCs, Route 53 VPC Resolver mulai memproses kueri DNS untuk mereka VPCs berdasarkan aturan yang tersisa. Perilaku akan sama seperti jika Anda memisahkan aturan dari VPC.

Jika aturan dibagikan ke Unit Organisasi (OU) dan akun di OU dipindahkan ke OU yang berbeda, semua asosiasi dengan aturan bersama ke VPC apa pun di akun akan dihapus. Namun, jika

aturan Resolver VPC sudah dibagikan dengan OU tujuan, maka asosiasi VPC akan tetap utuh dan tidak akan dipisahkan.

Jumlah maksimum aturan dan pengaitan

Ketika akun membuat aturan dan membagikannya dengan satu atau beberapa akun lain, jumlah maksimum aturan per AWS Wilayah berlaku untuk akun yang membuat aturan.

Ketika akun yang dibagikan aturan mengaitkan aturan dengan satu atau lebih VPCs, jumlah maksimum asosiasi antara aturan dan VPCs per Wilayah berlaku untuk akun tempat aturan tersebut dibagikan.

Untuk kuota Resolver VPC saat ini, lihat. [Kuota pada Route 53 VPC Resolver](#)

Izin

Untuk berbagi aturan dengan AWS akun lain, Anda harus memiliki izin untuk menggunakan [PutResolverRulePolicy](#) tindakan tersebut.

Pembatasan pada AWS akun tempat aturan dibagikan

Akun yang dibagikan aturan tidak dapat mengubah atau menghapus aturan.

Penandaan

Hanya akun yang membuat aturan yang dapat menambahkan, menghapus, atau melihat tanda pada aturan.

Untuk melihat status berbagi aturan saat ini (termasuk akun yang membagikan aturan atau akun tempat aturan dibagikan), dan untuk berbagi aturan dengan akun lain, lakukan prosedur berikut.

Untuk melihat status berbagi dan berbagi aturan dengan AWS akun lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat aturan.

Kolom Status berbagi menampilkan status berbagi aturan saat ini yang dibuat oleh akun saat ini atau yang dibagikan dengan akun saat ini:

- Tidak dibagikan: AWS Akun saat ini membuat aturan, dan aturan tidak dibagikan dengan akun lain.

- Dibagikan oleh saya: Akun saat ini membuat aturan dan membagikannya dengan satu atau beberapa akun.
 - Dibagikan dengan saya: Akun saat ini membuat aturan dan membagikannya dengan akun saat ini.
4. Pilih nama aturan dengan informasi berbagi yang ingin Anda tampilkan atau yang ingin Anda bagikan dengan akun lain.

Pada *rule name* halaman Aturan:, nilai di bawah Pemilik menampilkan ID akun yang membuat aturan. Itu adalah akun saat ini kecuali nilai Status berbagi adalah Dibagikan dengan saya. Dalam hal ini, Pemilik adalah akun yang membuat aturan dan membagikannya dengan akun saat ini.

5. Pilih Bagikan untuk melihat informasi tambahan atau berbagi aturan dengan akun lain. Halaman di konsol Resource Access Manager muncul, tergantung pada nilai Status berbagi:
- Tidak dibagikan: Halaman Buat berbagi sumber daya akan muncul. Untuk informasi tentang cara berbagi aturan dengan akun lain, OU, atau organisasi, lompat ke langkah 6.
 - Dibagikan oleh saya: Halaman Sumber daya bersama menampilkan aturan dan sumber daya lain yang dimiliki oleh akun saat ini dan dibagikan dengan akun lain.
 - Dibagikan dengan saya: Halaman Sumber daya bersama menampilkan aturan dan sumber daya lain yang dimiliki oleh akun lain dan dibagikan dengan akun saat ini.
6. Untuk berbagi aturan dengan AWS akun lain, OU, atau organisasi, tentukan nilai-nilai berikut.

 Note

Anda tidak dapat memperbarui pengaturan berbagi. Jika ingin mengubah salah satu pengaturan berikut, Anda harus membagikan ulang aturan dengan pengaturan baru lalu menghapus pengaturan berbagi yang lama.

Deskripsi

Masukkan deskripsi singkat yang membantu Anda mengingat alasan Anda berbagi aturan.

Sumber daya

Pilih kotak centang untuk aturan yang ingin Anda bagikan.

Pengguna utama

Masukkan nomor AWS akun, nama OU, atau nama organisasi.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Ini adalah tag yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda; Anda juga dapat menggunakan tag untuk tujuan lain. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Menggunakan tanda alokasi biaya](#) dalam Panduan Pengguna AWS Billing .

Menghapus aturan penerusan

Untuk menghapus aturan penerusan, lakukan prosedur berikut.

Perhatikan hal-hal berikut:

- Jika aturan penerusan dikaitkan dengan salah satu VPCs, Anda harus memisahkan aturan dari VPCs sebelum Anda dapat menghapus aturan. Untuk informasi selengkapnya, lihat [Memisahkan aturan penerusan dari VPC](#).
- Anda tidak dapat menghapus aturan Resolver Internet default, yang memiliki nilai Rekursif untuk Jenis. Aturan ini menyebabkan Route 53 VPC Resolver bertindak sebagai resolver rekursif untuk nama domain apa pun yang tidak Anda buat aturan kustom dan VPC Resolver tidak membuat aturan yang ditentukan secara otomatis. Untuk informasi selengkapnya tentang cara aturan dikategorikan, lihat [Menggunakan aturan untuk mengontrol kueri yang diteruskan ke jaringan Anda](#).

Cara menghapus aturan penerusan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat aturan.
4. Pilih opsi untuk aturan yang ingin Anda hapus.
5. Pilih Hapus.

6. Untuk mengonfirmasi bahwa Anda ingin menghapus aturan, masukkan nama aturan dan pilih Kirim.

Aturan penerusan untuk kueri DNS terbalik di VPC Resolver

Ketika `enableDnsHostnames` dan `enableDnsSupport` diatur ke `true` untuk virtual private cloud (VPC) dari Amazon VPC, VPC Resolver secara otomatis membuat aturan sistem yang ditentukan secara otomatis untuk kueri DNS terbalik. Untuk informasi selengkapnya tentang setelan ini, lihat [atribut DNS di VPC Anda di Panduan Pengembang Amazon VPC](#).

Aturan penerusan untuk kueri DNS terbalik sangat berguna untuk layanan seperti SSH atau Active Directory, yang memiliki opsi untuk mengautentikasi pengguna dengan melakukan pencarian DNS terbalik untuk alamat IP dari mana pelanggan mencoba untuk terhubung ke sumber daya. Untuk informasi selengkapnya tentang aturan sistem yang ditentukan secara otomatis, lihat [Nama domain yang VPC Resolver membuat aturan sistem yang ditentukan secara otomatis](#).

Anda dapat menonaktifkan aturan ini dan memodifikasi semua kueri DNS terbalik sehingga, misalnya, diteruskan ke server nama lokal Anda untuk resolusi.

Setelah Anda mematikan aturan otomatis, buat aturan untuk meneruskan kueri sesuai kebutuhan ke sumber daya lokal Anda. Untuk informasi selengkapnya tentang cara mengelola aturan penerusan, lihat [Mengelola aturan penerusan](#).

Untuk mematikan aturan yang ditentukan secara otomatis

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, di bawah VPC Resolver VPC pilih, lalu pilih ID VPC.
3. Di bawah Aturan yang ditentukan otomatis untuk resolusi DNS terbalik, batalkan centang pada kotak centang. Jika kotak centang sudah tidak dipilih, Anda dapat memilihnya untuk mengaktifkan resolusi DNS terbalik yang ditentukan secara otomatis.

Untuk yang terkait APIs, lihat Konfigurasi [VPC Resolver](#). APIs

Tutorial aturan delegasi penyelesai

Aturan delegasi memungkinkan Resolver VPC mencapai server nama yang menghosting zona yang didelegasikan melalui titik akhir keluar yang ditentukan. Sementara aturan penerusan

menginformasikan Resolver VPC untuk meneruskan kueri DNS ke server nama yang cocok dengan domain yang ditentukan melalui titik akhir keluar, aturan delegasi menginformasikan VPC Resolver untuk mencapai server nama yang didelegasikan melalui titik akhir keluar yang ditentukan saat catatan NS yang didelegasikan dikembalikan. VPC Resolver mengirimkan kueri ke server nama yang didelegasikan saat catatan NS dalam respons DNS cocok dengan nama domain yang ditentukan dalam catatan delegasi.

Langkah-langkah Menggunakan delegasi keluar titik akhir Resolver

1. Buat titik akhir keluar Resolver di VPC tempat Anda ingin kueri DNS berasal dari resolver di jaringan Anda.

Anda dapat menggunakan API berikut atau perintah CLI:

- [CreateResolverEndpointAPI](#)
- [create-resolver-endpointCLI](#)

2. Buat satu atau beberapa aturan delegasi, yang menentukan nama domain yang kueri harus didelegasikan ke jaringan Anda melalui titik akhir keluar yang ditentukan.

Contoh pembuatan aturan delegasi dengan CLI:

```
aws route53resolver create-resolver-rule \
--region REGION \
--creator-request-id delegateruletest \
--delegation-record example.com \
--name delegateruletest \
--rule-type DELEGATE \
--resolver-endpoint-id outbound endpoint ID
```

3. Kaitkan aturan delegasi dengan yang VPCs Anda inginkan kueri untuk didelegasikan.

Anda dapat menggunakan API berikut atau perintah CLI:

- [AssociateResolverRuleAPI](#).
- [associate-resolver-rules](#)Perintah CLI.

Jenis delegasi yang didukung oleh titik akhir keluar Resolver

VPC Resolver mendukung dua jenis delegasi keluar:

- Rutekan 53 zona host pribadi ke delegasi keluar VPC Resolver:

Mendelegasikan sub-domain dari zona host pribadi ke server DNS lokal atau zona yang dihosting publik di internet menggunakan delegasi keluar. Delegasi keluar ini memungkinkan Anda untuk membagi pengelolaan catatan DNS Anda antara zona host pribadi dan zona yang didelegasikan. Delegasi dapat dilakukan dengan atau tanpa catatan lem di zona host pribadi berdasarkan pengaturan DNS Anda. Untuk informasi lebih lanjut lihat [Zona host pribadi untuk keluar](#)

- VPC Resolver keluar ke delegasi keluar:

Mendelegasikan subdomain dari server DNS lokal Anda ke server lokal lain di lokasi yang sama atau berbeda menggunakan delegasi keluar ke luar. Ini mirip dengan mendelegasikan dari zona host pribadi ke titik akhir keluar, tempat Anda dapat mendelegasikan ke zona yang dihosting di server nama lokal Anda. Untuk mengetahui informasi selengkapnya, lihat [Keluar ke outbound](#).

Rutekan 53 zona host pribadi ke konfigurasi contoh delegasi keluar VPC Resolver

Mari kita asumsikan pengaturan DNS di mana zona host induk dihosting di zona host pribadi Route 53 di VPC Amazon dan subdomain didelegasikan ke server nama yang dihosting di Eropa, Asia, dan Amerika Utara. Semua kueri DNS dilewatkan melalui VPC Resolver.

Ikuti langkah-langkah contoh untuk mengonfigurasi zona host pribadi dan Resolver VPC Anda.

Konfigurasi zona host pribadi untuk delegasi keluar

1. Untuk pengaturan zona yang dihosting pribadi:

Zona yang dihosting orang tua: `hr.example.com`

```
$TTL      86400 ; 24 hours
$ORIGIN hr.example.com
@ 1D IN    SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN    NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of Zone Delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue Record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue Record
```

2. Untuk server nama lokal di wilayah lokal Eropa:

- Zona yang Dihosting: eu.hr.example.com NS IP: 10.0.0.30

```
$TTL      86400 ; 24 hours
$ORIGIN eu.hr.example.com
@ 1D IN    SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN    NS @
test.eu.hr.example.com IN A 1.2.3.4
```

3. Untuk server nama lokal di wilayah lokal Asia:

Zona yang Dihosting: apac.hr.example.com, 10.0.0.40

Server nama apac dapat mendelegasikan subdomain ke server nama lain.

```
$TTL      86400 ; 24 hours
$ORIGIN apac.hr.example.com
@ 1D IN    SOA @      root (20200322001 3H 15 1w 3h)
@ 1D IN    NS @
test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

Zona yang Dihosting: engineering.apac.hr.example.com, 10.0.0.80

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. Untuk server nama lokal di wilayah lokal Amerika Utara:

Zona yang Dihosting: na.hr.example.net NS IP: 10.0.0.50

```
$TTL      86400 ; 24 hours
$ORIGIN na.hr.example.net
```

```
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com IN A 9.10.11.12
```

Pengaturan VPC Resolver

- Untuk Resolver VPC, Anda perlu menyiapkan satu aturan penerusan dan dua aturan delegasi:

Aturan maju

- Untuk meneruskan catatan out-of-zone delegasi, sehingga Route 53 VPC Resolver mengetahui IP dari NS yang didelegasikan untuk meneruskan permintaan awal.

nama domain: target-ips: `hr.example.net 10.0.0.50`

Aturan delegasi

- Aturan delegasi untuk delegasi dalam zona:

catatan delegasi: `hr.example.com`

- Aturan delegasi untuk delegasi di luar zona:

catatan delegasi: `hr.example.net`

Konfigurasi contoh delegasi keluar ke luar

Alih-alih memiliki zona host induk di VPC Amazon, mari kita asumsikan penyiapan DNS di mana zona host induk berada di lokasi lokal pusat dan subdomain sedang didelegasikan ke server nama yang dihosting di Eropa, Asia, dan Amerika Utara. Semua kueri DNS dilewatkan melalui VPC Resolver.

Ikuti contoh langkah untuk mengonfigurasi DNS lokal dan Resolver VPC Anda.

Konfigurasi DNS di lokasi

- Untuk server nama lokal di wilayah lokal pusat:

- Zona yang dihosting orang tua: `hr.example.com`

Zona yang Dihosting `hr.example.com`, NS IP: `10.0.0.20`

```
$TTL      86400 ; 24 hours
$ORIGIN hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of zone delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue record
```

2. Untuk server nama lokal di wilayah lokal Eropa (konfigurasi untuk server nama Eropa, Asia, dan Amerika Utara sama dengan zona host pribadi ke delegasi keluar):

- Zona yang Dihosting: eu.hr.example.com NS IP: 10.0.0.30

```
$TTL      86400 ; 24 hours
$ORIGIN eu.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. Untuk server nama lokal di wilayah lokal Asia:

Zona yang Dihosting: apac.hr.example.com, 10.0.0.40

Server nama apac dapat mendelegasikan subdomain ke server nama lain.

```
$TTL      86400 ; 24 hours
$ORIGIN apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

Zona yang Dihosting: `engineering.apac.hr.example.com`, `10.0.0.80`

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. Untuk server nama lokal di wilayah lokal Amerika Utara:

Zona yang Dihosting: `na.hr.example.net` NS IP: `10.0.0.50`

```
$TTL 86400 ; 24 hours
$ORIGIN na.hr.example.net
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com IN A 9.10.11.12
```

Pengaturan VPC Resolver

- Untuk Resolver VPC, Anda perlu mengatur aturan penerusan dan aturan delegasi:

Aturan maju

1. Untuk meneruskan permintaan awal sehingga kueri akan diteruskan ke zona `hr.example.com` host induk di lokasi pusat:

nama domain: `target-ips: hr.example.com 10.0.0.20`

2. Untuk meneruskan catatan out-of-zone delegasi, sehingga VPC Resolver mengetahui alamat IP server nama yang didelegasikan untuk meneruskan permintaan awal:

nama domain: `target-ips: hr.example.net 10.0.0.50`

Aturan delegasi

1. Aturan delegasi untuk delegasi dalam zona:

catatan delegasi: `hr.example.com`

2. Aturan Delegasi untuk delegasi di luar zona:

catatan delegasi: `hr.example.net`

Mengaktifkan validasi DNSSEC di Amazon Route 53

Saat Anda mengaktifkan validasi DNSSEC untuk virtual private cloud (VPC) di Amazon Route 53, tanda tangan DNSSEC diperiksa secara kriptografis untuk memastikan bahwa respons tidak dirusak. Anda mengaktifkan validasi DNSSEC di halaman detail VPC.

Validasi DNSSEC diterapkan oleh VPC Resolver ke nama yang ditandatangani publik saat melakukan resolusi DNS rekursif.

Namun, jika Resolver VPC meneruskan ke resolver DNS lain, resolver tersebut melakukan resolusi DNS rekursif dan, oleh karena itu, juga harus menerapkan validasi DNSSEC.

Important

Mengaktifkan validasi DNSSEC dapat memengaruhi resolusi DNS untuk data DNS publik dari sumber daya AWS dalam VPC, yang dapat mengakibatkan pemadaman. Perhatikan bahwa mengaktifkan atau menonaktifkan validasi DNSSEC dapat memakan waktu beberapa menit.

Note

Pada saat ini, Route 53 VPC Resolver di VPC Anda (alias AmazonProvided DNS) mengabaikan bit header DO (DNSSEC OK) EDNS dan bit CD (Checking Disabled) dalam kueri DNS. Jika Anda telah mengonfigurasi DNSSEC, ini berarti bahwa sementara VPC Resolver melakukan validasi DNSSEC, DNSSEC tidak mengembalikan catatan DNSSEC atau mengatur bit AD dalam respons. Oleh karena itu, melakukan validasi DNSSEC Anda sendiri saat ini tidak didukung oleh VPC Resolver. Jika Anda perlu melakukan ini, Anda harus melakukan resolusi DNS rekursif Anda sendiri.

Cara mengaktifkan validasi DNSSEC untuk VPC

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

2. Di panel navigasi, di bawah VPC Resolver, pilih. VPCs
3. Di bawah validasi DNSSEC, pilih kotak centang. Jika kotak centang sudah dipilih, Anda dapat menghapusnya untuk menonaktifkan validasi DNSSEC.

Perhatikan bahwa mengaktifkan atau menonaktifkan validasi DNSSEC dapat memakan waktu beberapa menit.

Merutekan lalu lintas internet ke sumber daya Anda AWS

Anda dapat menggunakan Amazon Route 53 untuk merutekan lalu lintas ke berbagai AWS sumber daya.

- [Merutekan lalu lintas ke API Amazon API Gateway dengan menggunakan nama domain Anda](#)
- [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#)
- [Merutekan lalu lintas ke instans Amazon EC2](#)
- [Merutekan lalu lintas ke layanan AWS App Runner](#)
- [Routing lalu lintas ke AWS Global Accelerator](#)
- [Merutekan lalu lintas ke lingkungan AWS Elastic Beanstalk](#)
- [Merutekan lalu lintas ke penyeimbang beban ELB](#)
- [Merutekan lalu lintas ke situs web yang di-host di bucket Amazon S3](#)
- [Merutekan lalu lintas ke titik akhir antarmuka Amazon Virtual Private Cloud dengan menggunakan nama domain Anda](#)
- [Merutekan lalu lintas ke Amazon WorkMail](#)
- [Merutekan lalu lintas ke titik akhir domain OpenSearch Layanan Amazon](#)
- [Merutekan lalu lintas ke titik akhir domain layanan Amazon VPC Lattice](#)
- [Merutekan lalu lintas ke sumber daya lain AWS](#)
- [Membuat sumber daya Amazon Route 53 dan Route 53 VPC Resolver dengan AWS CloudFormation](#)

Merutekan lalu lintas ke API Amazon API Gateway dengan menggunakan nama domain Anda

Anda dapat menggunakan Amazon API Gateway untuk membuat, menerbitkan, memelihara, memantau, dan mengamankan APIs. Anda dapat membuat AWS layanan akses APIs tersebut atau layanan web lainnya selain data yang disimpan di AWS Cloud.

Metode yang Anda gunakan untuk merutekan lalu lintas domain ke API pada API Gateway adalah sama terlepas dari apakah Anda membuat titik akhir API Gateway regional atau titik akhir API Gateway yang dioptimalkan edge. Jika Anda membuat titik akhir API Gateway pribadi, prosesnya sedikit berbeda.

- Titik akhir API Regional: Anda membuat catatan alias Route 53 yang merutekan lalu lintas ke titik akhir API regional.
- Titik akhir API yang dioptimalkan edge: Anda membuat catatan alias Route 53 yang merutekan lalu lintas ke API yang dioptimalkan edge. Hal ini menyebabkan lalu lintas dialihkan ke CloudFront distribusi yang terkait dengan API yang dioptimalkan tepi.
- Titik akhir API pribadi: Anda membuat catatan alias Route 53 yang merutekan lalu lintas ke titik akhir API pribadi Anda menggunakan titik akhir VPC antarmuka untuk API Gateway di zona host pribadi.

Catatan alias adalah ekstensi Route 53 ke DNS yang mirip dengan data CNAME. Untuk perbandingan alias dan data CNAME, lihat [Memilih antara catatan alias dan nonalias](#).

Note

Route 53 tidak mengenakan biaya untuk kueri alias ke API Gateway APIs atau sumber daya lainnya AWS .

Topik

- [Prasyarat](#)
- [Mengonfigurasi Route 53 untuk merutekan lalu lintas ke titik akhir API Gateway](#)

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- API Gateway API yang memiliki nama domain khusus, seperti api.example.com yang cocok dengan nama record Route 53 yang ingin Anda buat.

Untuk informasi selengkapnya, lihat topik berikut:

- [Menyiapkan nama domain khusus untuk HTTP APIs](#) di Panduan Pengembang Amazon API Gateway.
- [Menyiapkan nama domain khusus untuk REST APIs](#) di Panduan Pengembang Amazon API Gateway.
- [Menyiapkan nama domain khusus untuk WebSocket APIs](#) di Panduan Pengembang Amazon API Gateway.

- [Nama domain khusus untuk pribadi APIs di API Gateway](#) di Panduan Pengembang Amazon API Gateway.
- Nama domain terdaftar. Anda dapat menggunakan Amazon Route 53 sebagai pencatat domain Anda atau Anda dapat menggunakan registrar lain.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengonfigurasi Route 53 untuk merutekan lalu lintas ke titik akhir API Gateway

Untuk mengonfigurasi Route 53 untuk merutekan lalu lintas ke titik akhir API Gateway, lakukan prosedur berikut.

Custom domain names for public APIs

Prosedur berikut menjelaskan cara merutekan lalu lintas ke titik akhir API Gateway untuk nama domain khusus untuk publik APIs.

Untuk merutekan lalu lintas ke titik akhir API Gateway

1. Jika Anda membuat zona yang di-hosting Route 53 dan titik akhir menggunakan akun yang sama, lewati ke langkah 2.

Jika Anda membuat zona yang di-hosting dan titik akhir menggunakan akun yang berbeda, dapatkan nama domain target untuk nama domain khusus yang ingin Anda gunakan:

- a. Masuk ke Konsol Manajemen AWS dan buka konsol API Gateway di <https://console.aws.amazon.com/apigateway/>.
 - b. Di panel navigasi, pilih Custom domain names (Nama domain khusus).
 - c. Pilih nama domain kustom yang ingin Anda gunakan dan dapatkan nilai nama domain API Gateway.
2. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 3. Di panel navigasi, pilih Hosted zones (Zona yang di-hosting).

4. Pilih nama zona yang di-hosting yang memiliki nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke API Anda.
5. Pilih Create record (Buat catatan).
6. Tentukan nilai-nilai berikut ini:

 Important

Kami menyarankan Anda mengaktifkan Alias. Untuk nama domain yang tidak menggunakan catatan Alias Route 53, Anda mungkin mengalami masalah jika menggunakan VPC dengan DNS pribadi yang diaktifkan untuk menjalankan API pribadi. DNS pribadi mengganti perilaku resolusi DNS default dalam VPC, yang dapat menyebabkan konflik dengan catatan DNS eksternal.

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke API Anda.

API yang ingin Anda rutekan lalu lintas harus menyertakan nama domain khusus, seperti `api.example.com` yang cocok dengan nama catatan Route 53.

Alias

Jika Anda menggunakan metode pembuatan catatan Pembuatan cepat, aktifkan Alias.

Menilai/Merutekan lalu lintas

Pilih Alias to API Gateway API (Alias ke API Gateway API), lalu pilih Wilayah tempat titik akhir berasal.

Cara Anda menentukan nilai untuk Endpoint bergantung pada apakah Anda membuat zona yang dihosting dan API menggunakan akun yang sama atau AWS akun yang berbeda:

- Akun yang sama — Daftar nama domain target hanya mencakup APIs yang memiliki nama domain khusus yang cocok dengan nilai yang Anda tentukan untuk nama Rekam. Pilih nilai yang sesuai.
- Akun yang berbeda – Masukkan nilai yang Anda dapatkan pada langkah 1 dari prosedur ini.

Tipe catatan

Pilih A — IPv4 alamat.

Mengevaluasi Kondisi Target

Untuk kontrol atas failover DNS, konfigurasi pemeriksaan kesehatan khusus. Sebagai contoh, lihat [Mengonfigurasi pemeriksaan kesehatan khusus untuk failover DNS](#) di panduan pengguna API Gateway.

7. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Saat propagasi selesai, Anda akan dapat merutekan lalu lintas ke API Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Custom domain names for private APIs

Prosedur berikut menjelaskan cara merutekan lalu lintas ke titik akhir API Gateway untuk nama domain kustom untuk pribadi APIs.

Untuk merutekan lalu lintas ke titik akhir API Gateway

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama zona host pribadi yang memiliki nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke API Anda.
4. Pilih Create record (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke API Anda.

API yang ingin Anda rutekan lalu lintas harus menyertakan nama domain khusus, seperti `api.example.com` yang cocok dengan nama catatan Route 53.

Alias

Nyalakan Alias.

Nilai/Rutekan lalu lintas ke

Pilih Alias ke VPC Endpoint. Pilih Wilayah tempat titik akhir berasal, lalu pilih titik akhir VPC Anda.

Tipe catatan

Jika Anda menggunakan IPv6 untuk titik akhir VPC Anda, buat jenis catatan AAAA. Jika Anda menggunakan dualstack untuk titik akhir VPC Anda, buat AAAA dan tipe catatan A.

Mengevaluasi Kondisi Target

Untuk kontrol atas failover DNS, konfigurasi pemeriksaan kesehatan khusus. Sebagai contoh, lihat [Mengonfigurasi pemeriksaan kesehatan khusus untuk failover DNS](#) di panduan pengguna API Gateway.

6. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Saat propagasi selesai, Anda akan dapat merutekan lalu lintas ke API Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda

Topik ini menyediakan prosedur komprehensif untuk merutekan lalu lintas DNS ke distribusi Amazon CloudFront apa pun. Jika Anda menyiapkan situs web statis dengan Amazon CloudFront dan Amazon Simple Storage Service, lihat [Gunakan CloudFront distribusi Amazon untuk melayani situs web statis](#) tutorial lengkapnya.

Anda dapat menggunakan Amazon CloudFront, jaringan pengiriman AWS konten (CDN), sebagai salah satu cara untuk mempercepat pengiriman konten web Anda. CloudFront dapat mengirimkan seluruh situs web Anda — termasuk konten dinamis, statis, streaming, dan interaktif — dengan menggunakan jaringan global lokasi tepi. Pengguna yang meminta konten Anda secara otomatis diarahkan ke lokasi tepi yang memberi mereka latensi terendah.

 Note

Anda dapat merutekan lalu lintas ke CloudFront distribusi hanya untuk zona yang dihosting publik.

Untuk digunakan CloudFront untuk mendistribusikan konten situs web Anda, buat distribusi dan tentukan pengaturan untuk itu. Misalnya, tentukan bucket Amazon S3 atau server HTTP tempat Anda CloudFront ingin mendapatkan konten, apakah Anda hanya ingin pengguna terpilih yang memiliki akses ke konten Anda, dan apakah Anda ingin pengguna menggunakan HTTPS.

Saat Anda membuat distribusi, CloudFront tetapkan nama domain ke distribusi, seperti `d111111abcdef8.cloudfront.net`. Anda dapat menggunakan nama domain ini di URLs untuk konten Anda, misalnya:

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

Atau, Anda dapat menggunakan nama domain Anda sendiri di URLs, misalnya:

```
http://example.com/logo.jpg
```

Ikuti langkah-langkah dalam Panduan CloudFront Pengembang Amazon untuk menggunakan nama domain Anda sendiri di file Anda URLs dalam CloudFront distribusi, bukan nama domain yang ditetapkan CloudFront untuk distribusi Anda. Untuk informasi selengkapnya, tentang menggunakan nama domain Anda sendiri dengan CloudFront distribusi, lihat [Menggunakan kustom URLs dengan menambahkan nama domain alternatif \(CNAMEs\)](#).

Saat Anda menggunakan nama domain Route 53 dengan CloudFront distribusi, gunakan Amazon Route 53 untuk membuat [catatan alias](#) yang mengarah ke CloudFront distribusi Anda. Catatan alias adalah ekstensi Route 53 ke DNS. Ini mirip dengan data CNAME, tetapi Anda dapat membuat data alias untuk domain akar, seperti `example.com`, dan untuk subdomain, seperti `www.example.com`. (Anda dapat membuat data CNAME hanya untuk subdomain.) Saat Route 53 menerima kueri DNS yang cocok dengan nama dan tipe catatan alias, Route 53 merespons dengan nama domain yang terkait dengan distribusi Anda.

 Note

Route 53 tidak mengenakan biaya untuk kueri alias ke CloudFront distribusi atau sumber daya lainnya. AWS

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

1. Nama domain terdaftar. Anda dapat menggunakan Amazon Route 53 sebagai pencatat domain Anda atau Anda dapat menggunakan registrar lain.
2. Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

3. Penyewa CloudFront distribusi atau CloudFront distribusi. Distribusi harus menyertakan nama domain alternatif yang cocok dengan nama domain yang ingin Anda gunakan untuk Anda, URLs bukan nama domain yang CloudFront ditetapkan untuk distribusi Anda. Untuk penyewa CloudFront distribusi, itu harus berisi nama domain yang ingin Anda gunakan untuk Anda URLs.

Misalnya, jika Anda ingin konten Anda berisi nama domain example.com, bidang Nama Domain Alternatif untuk distribusi harus menyertakan example.com. URLs

Untuk informasi selengkapnya, lihat dokumentasi berikut di Panduan CloudFront Pengembang Amazon:

- [Daftar tugas untuk membuat distribusi](#)
- [Membuat atau memperbarui distribusi menggunakan CloudFront konsol](#)

 Note

Jika Anda membuat situs web statis, lihat [Memulai situs web statis aman](#) di Panduan CloudFront Pengembang Amazon untuk petunjuk penyiapan lengkap.

4. (Opsional) Minta sertifikat publik sehingga CloudFront distribusi Amazon memerlukan HTTPS. Untuk informasi selengkapnya, lihat [Validasi DNS AWS Certificate Manager di AWS Certificate Manager](#) Panduan Pengguna.

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke distribusi CloudFront

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke CloudFront distribusi, ikuti langkah-langkah berikut. Untuk informasi selengkapnya tentang menggunakan nama domain Anda sendiri dengan CloudFront distribusi, lihat [Menggunakan kustom URLs dengan menambahkan nama domain alternatif \(CNAMEs\)](#) di Panduan CloudFront Pengembang Amazon.

Note

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Ketika perubahan menyebar, Anda akan dapat merutekan lalu lintas ke CloudFront distribusi Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Untuk merutekan lalu lintas ke CloudFront distribusi

1. Dapatkan nama domain yang CloudFront ditetapkan untuk distribusi Anda dan tentukan IPv6 apakah diaktifkan:
 - a. Masuk ke Konsol Manajemen AWS dan buka CloudFront konsol di <https://console.aws.amazon.com/cloudfront/v4/home>.
 - b. di kolom ID, pilih nama terkait distribusi yang ingin Anda rute lalu lintas ke (bukan kotak centang).
 - c. Pada tab General, dapatkan nilai bidang Distribution domain name.
 - d. Pada tab Umum, di bagian Pengaturan, pilih edit dan gulir untuk memeriksa IPv6 bidang untuk melihat IPv6 apakah diaktifkan untuk distribusi. Jika IPv6 diaktifkan, Anda harus membuat dua catatan alias untuk distribusi, satu untuk merutekan IPv4 lalu lintas ke distribusi, dan satu untuk merutekan IPv6 lalu lintas. Pilih Batalkan.

Untuk informasi selengkapnya, lihat [Mengaktifkan IPv6](#) dalam topik [Nilai yang Anda tentukan saat membuat atau memperbarui distribusi](#) di Panduan CloudFront Pengembang Amazon.

2. Untuk penyewa CloudFront distribusi,
 - a. Pilih SaaS di navigasi kiri, lalu Penyewa distribusi, dan pilih penyewa distribusi dengan nama domain yang ingin Anda rutekan lalu lintas
 - b. di bagian Rincian umum, salin nilai Titik Akhir.
3. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
4. Pada panel navigasi, pilih Zona yang di-hosting.
5. Pilih nama yang ditautkan dari zona yang dihosting untuk domain yang ingin Anda gunakan untuk merutekan lalu lintas ke CloudFront distribusi Anda.
6. Pilih Create record (Buat catatan).
7. Tentukan nilai-nilai berikut ini:

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk mengarahkan lalu lintas ke CloudFront distribusi Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk mengarahkan lalu lintas ke distribusi Anda, masukkan acme.

Tipe catatan

Pilih A — IPv4 alamat.

Jika IPv6 diaktifkan untuk distribusi dan Anda membuat rekaman kedua, pilih AAAA — IPv6 alamat.

Alias

Nyalakan Alias.



Important

Anda harus membuat catatan Alias agar CloudFront distribusi berfungsi.

Rute lalu lintas ke

Pilih Alias untuk CloudFront didistribusikan. Pilih nama domain yang CloudFront ditetapkan untuk distribusi saat Anda membuatnya. Ini adalah nilai yang Anda dapatkan di langkah 1.

Untuk penyewa CloudFront distribusi, pilih titik akhir dari langkah 2.

Mengevaluasi Kondisi Target

Terima nilai default Tidak.

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

8. Pilih Create records (Buat catatan).
9. Jika IPv6 diaktifkan untuk distribusi, ulangi langkah 5 hingga 7. Tentukan pengaturan yang sama kecuali untuk bidang Jenis rekaman, seperti yang dijelaskan pada langkah 6.

Merutekan lalu lintas ke instans Amazon EC2

Amazon EC2 menyediakan kapasitas komputasi yang dapat diskalakan di AWS Cloud. Anda dapat meluncurkan lingkungan komputasi EC2 virtual (instance) menggunakan templat yang telah dikonfigurasi sebelumnya (Amazon Machine Image atau AMI). Ketika Anda meluncurkan EC2 instans, EC2 secara otomatis menginstal sistem operasi (Linux atau Microsoft Windows) dan perangkat lunak tambahan yang disertakan dalam AMI, seperti server web atau perangkat lunak database.

Anda dapat merutekan lalu lintas untuk domain Anda, seperti example.com, ke server Anda dengan menggunakan Amazon Route 53, jika Anda menghosting situs web atau menjalankan aplikasi web pada sebuah EC2 instans.

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- EC2 Contoh Amazon. Untuk informasi tentang meluncurkan EC2 instance, lihat dokumentasi berikut:

- Linux — Lihat [Memulai instans Amazon EC2 Linux](#) di EC2 Panduan Pengguna Amazon
- Microsoft Windows - Lihat [Memulai instans Amazon EC2 Windows](#) di EC2 Panduan Pengguna Amazon

⚠ Important

Kami menyarankan Anda juga membuat [alamat IP Elastis](#) dan mengaitkannya dengan EC2 instans Anda. Alamat IP Elastis memastikan bahwa alamat IP EC2 instans Amazon Anda tidak akan pernah berubah. Untuk informasi yang berkaitan dengan harga, lihat [Harga untuk alamat IP elastis](#).

- Nama domain terdaftar. Anda dapat menggunakan Amazon Route 53 sebagai pencatat domain Anda atau Anda dapat menggunakan registrar lain.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke instans Amazon EC2

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke EC2 instans, lakukan prosedur berikut.

Untuk merutekan lalu lintas ke EC2 instans Amazon

1. Dapatkan alamat IP untuk EC2 instans Amazon:
 - a. Masuk ke Konsol Manajemen AWS dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
 - b. Di daftar Wilayah di sudut kanan atas konsol, pilih Wilayah tempat Anda meluncurkan instans.
 - c. Di panel navigasi, pilih Instances (Instans).
 - d. Di tabel, pilih instans yang ingin Anda rutekan lalu lintasnya.

- e. Di panel bawah, pada tab Deskripsi, dapatkan nilai IPsElastis.

Jika Anda tidak mengaitkan IP Elastis dengan instance, dapatkan nilai IP IPv4 Publik.

2. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Pada panel navigasi, pilih Zona yang di-hosting.
4. Pilih nama zona yang di-hosting yang sesuai dengan nama domain yang ingin Anda rutekan lalu lintasnya.
5. Pilih Create record (Buat catatan).
6. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke EC2 instans Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang dihosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke instance Anda, masukkan acme. EC2

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan). Masukkan alamat IP yang Anda dapatkan di langkah 1.

Tipe catatan

Pilih A — IPv4 alamat.

TTL (detik)

Terima nilai default 300.

7. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Ketika propagasi selesai, Anda akan dapat merutekan lalu lintas ke EC2 instans Anda dengan menggunakan nama catatan yang Anda buat dalam prosedur ini.

 Important

Jika Anda melepaskan IP elastis, pastikan Anda juga menghapus catatan DNS yang menunjuk ke sana. Jika tidak, Anda akan memiliki catatan DNS menggantung yang dapat diambil alih oleh pengguna yang tidak sah.

Merutekan lalu lintas ke layanan AWS App Runner

AWS App Runner adalah layanan yang dikelola sepenuhnya yang memudahkan pengembang untuk menyebarkan aplikasi web dalam peti kemas dan dalam skala besar dan APIs tanpa memerlukan pengalaman infrastruktur sebelumnya. Mulailah dengan kode sumber Anda atau gambar kontainer. App Runner membangun dan menyebarkan aplikasi web secara otomatis, memuat saldo lalu lintas dengan enkripsi, skala untuk memenuhi kebutuhan lalu lintas Anda, dan memudahkan layanan Anda untuk berkomunikasi dengan AWS layanan dan aplikasi lain yang berjalan di VPC Amazon pribadi. Dengan App Runner, daripada memikirkan server atau penskalaan, Anda memiliki lebih banyak waktu untuk fokus pada aplikasi Anda. Untuk informasi selengkapnya, lihat [Apa yang ada AWS App Runner](#) di Panduan AWS App Runner Pengembang.

 Important

Amazon Route 53 saat ini mendukung catatan alias untuk AWS App Runner layanan yang dibuat setelah 1 Agustus 2022.

Untuk merutekan traffic domain ke App Runner Service, gunakan Amazon Route 53 untuk membuat [rekaman alias](#) yang mengarah ke layanan App Runner Anda. Catatan alias adalah ekstensi Route 53 ke DNS. Ini mirip dengan catatan CNAME, kecuali Anda dapat membuat catatan alias baik untuk domain root, seperti example.com, dan untuk subdomain, seperti www.example.com (http://www.example.com/). Anda hanya dapat membuat catatan CNAME untuk subdomain.

 Note

Route 53 tidak mengenakan biaya untuk kueri alias ke layanan App Runner atau sumber daya lainnya. AWS

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- Layanan Pelari Aplikasi. Untuk informasi tentang membuat layanan App Runner, lihat [Memulai App Runner](#).
- Nama domain terdaftar. Anda dapat menggunakan Amazon Route 53 sebagai registrar domain Anda, atau Anda dapat menggunakan registrar yang berbeda.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

- Mengaitkan domain kustom ke layanan App Runner Anda. Untuk informasi selengkapnya, lihat [Mengelola nama domain khusus untuk App Runner](#).
- Konfigurasi catatan validasi sertifikat yang dikembalikan oleh App Runner ke zona host Route 53 Anda untuk memulai proses validasi domain. Untuk informasi selengkapnya, lihat [Validasi DNS AWS Certificate Manager di AWS Certificate Manager](#) Panduan Pengguna.

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke layanan App Runner

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke layanan App Runner, lakukan prosedur berikut.

Untuk merutekan lalu lintas ke layanan App Runner

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama zona yang di-hosting yang sesuai dengan nama domain yang ingin Anda rutekan lalu lintasnya.
4. Pilih Create record (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke layanan App Runner Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang dihosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke layanan App Runner, masukkan acme.

Nilai/Rutekan lalu lintas ke

Pilih Alias ke Layanan Pelari Aplikasi, lalu pilih. Wilayah AWS Pilih nama domain lingkungan tempat Anda ingin merutekan lalu lintas.

Tipe catatan

Terima nilai default, A — IPv4 alamat.

Mengevaluasi Kondisi Target

Pilih No. Untuk informasi tentang mengevaluasi kesehatan target, lihat [Mengevaluasi Kondisi Target](#).

6. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Ketika propagasi selesai, Anda akan dapat merutekan lalu lintas ke layanan App Runner Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Routing lalu lintas ke AWS Global Accelerator

AWS Global Accelerator adalah layanan di mana Anda membuat akselerator untuk meningkatkan kinerja aplikasi Anda untuk pengguna lokal dan global. Layanan bereaksi langsung terhadap perubahan kesehatan atau konfigurasi untuk memastikan bahwa lalu lintas internet dari klien selalu diarahkan ke titik akhir yang sehat. Global Accelerator mencakup arsitektur toleran kesalahan, dan menggabungkan AWS Shield Standard, untuk mitigasi in-line otomatis dari serangan S. DDo Untuk informasi selengkapnya, lihat [Apa itu Akselerator Global](#) di Panduan AWS Global Accelerator Pengembang.

Secara default, Global Accelerator memberi Anda alamat IP statis yang Anda kaitkan dengan akselerator Anda. Alamat IP statis adalah anycast dari jaringan AWS edge. Akselerator menyertakan nama DNS tuli, tetapi dalam sebagian besar skenario, Anda dapat mengonfigurasi DNS untuk menggunakan nama domain kustom Anda (seperti www.example.com) dengan akselerator Anda, alih-alih menggunakan alamat IP statis yang ditetapkan atau nama DNS default.

Note

Route 53 tidak mengenakan biaya untuk kueri alias ke Global Accelerator atau sumber daya lainnya. AWS

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- Akselerator. Anda dapat membuat akselerator standar, atau akselerator perutean khusus. Untuk informasi selengkapnya, lihat [Membuat akselerator standar dan Membuat akselerator perutean kustom](#).
- Nama domain terdaftar. Anda dapat menggunakan Amazon Route 53 sebagai registrar domain Anda, atau Anda dapat menggunakan registrar yang berbeda.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke akselerator

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke akselerator, lakukan prosedur berikut.

Untuk merutekan lalu lintas ke akselerator

1. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama zona yang di-hosting yang sesuai dengan nama domain yang ingin Anda rutekan lalu lintasnya.
4. Pilih Create record (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk mengarahkan lalu lintas ke akselerator Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang dihosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke Akselerator Global Anda, masukkan acme.

Nilai/Rutekan lalu lintas ke

Pilih Alias ke Global Accelerator, lalu pilih. Wilayah AWS Pilih nama DNS untuk akselerator.

Anda dapat memasukkan nama DNS akselerator yang Anda buat menggunakan arus Akun AWS atau menggunakan yang berbeda. Akun AWS

Tipe catatan

Terima nilai default, A — IPv4 alamat.

Mengevaluasi kondisi target

Terima nilai default Ya.

6. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Ketika propagasi selesai, Anda akan dapat merutekan lalu lintas ke akselerator Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Merutekan lalu lintas ke lingkungan AWS Elastic Beanstalk

Jika Anda menggunakan AWS Elastic Beanstalk untuk menyebarkan dan mengelola aplikasi di AWS Cloud, Anda dapat menggunakan Amazon Route 53 untuk merutekan lalu lintas DNS untuk domain Anda, seperti example.com, ke lingkungan Elastic Beanstalk baru atau yang sudah ada.

Untuk merutekan lalu lintas DNS ke lingkungan Elastic Beanstalk, lihat prosedur dalam topik berikut.

Note

Prosedur ini mengasumsikan bahwa Anda sudah menggunakan Route 53 sebagai layanan DNS untuk domain Anda. Jika Anda menggunakan layanan DNS lain, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#) untuk informasi tentang penggunaan Route 53 sebagai penyedia layanan DNS untuk domain Anda.

Topik

- [Men-deploy aplikasi ke lingkungan Elastic Beanstalk](#)
- [Mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda](#)
- [Membuat catatan Amazon Route 53 yang merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda](#)

Men-deploy aplikasi ke lingkungan Elastic Beanstalk

Jika Anda sudah memiliki lingkungan Elastic Beanstalk yang ingin Anda rutekan lalu lintasnya, lewati ke [Mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda](#).

Untuk membuat aplikasi dan menerapkannya ke lingkungan Elastic Beanstalk

- Untuk informasi tentang membuat aplikasi dan menyebarkannya ke lingkungan Elastic Beanstalk, lihat [Memulai menggunakan Elastic Beanstalk](#) di Panduan Developer AWS Elastic Beanstalk .

Mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda

Jika Anda sudah tahu nama domain untuk lingkungan Elastic Beanstalk Anda, lewati ke [Membuat catatan Amazon Route 53 yang merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda](#).

Untuk mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Elastic Beanstalk di <https://console.aws.amazon.com/elasticbeanstalk/>
2. Dalam daftar aplikasi, temukan aplikasi yang ingin Anda rutekan lalu lintasnya, dan dapatkan nilai URL. Jika Anda tidak melihat daftar aplikasi, pilih Aplikasi di panel navigasi.

Untuk informasi selengkapnya tentang URL, lihat nama domain [lingkungan Elastic Beanstalk di Panduan Pengembang Elastic Beanstalk](#).

Membuat catatan Amazon Route 53 yang merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda

Catatan Amazon Route 53 berisi pengaturan yang mengontrol bagaimana lalu lintas dirutekan ke lingkungan Elastic Beanstalk Anda. Anda membuat catatan CNAME atau catatan alias, bergantung pada apakah nama domain untuk lingkungan menyertakan Wilayah, seperti us-east-2, tempat Anda men-deploy lingkungan. Lingkungan baru menyertakan Wilayah dalam nama domain; lingkungan yang dibuat sebelum awal 2016 tidak. Untuk perbandingan data CNAME dan alias, lihat [Memilih antara catatan alias dan nonalias](#).

Jika nama domain tidak menyertakan Wilayah

Anda harus membuat catatan CNAME. Namun, karena batasan yang diberlakukan oleh DNS, Anda dapat membuat catatan CNAME hanya untuk subdomain, bukan untuk nama domain root. Misalnya, jika nama domain Anda adalah example.com, Anda dapat membuat catatan yang merutekan lalu lintas untuk acme.example.com ke lingkungan Elastic Beanstalk Anda, tetapi Anda tidak dapat membuat catatan yang merutekan lalu lintas untuk example.com ke lingkungan Elastic Beanstalk Anda.

Lihat prosedur [Untuk membuat catatan CNAME untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk](#).

Jika nama domain menyertakan Wilayah

Anda dapat membuat catatan alias. Catatan alias khusus untuk Route 53 dan memiliki dua keunggulan signifikan dibandingkan catatan CNAME:

- Anda dapat membuat catatan alias untuk nama domain root atau untuk subdomain. Misalnya, jika nama domain Anda adalah example.com, Anda dapat membuat catatan yang mengarahkan permintaan untuk example.com atau acme.example.com ke lingkungan Elastic Beanstalk Anda.

- Route 53 tidak mengenakan biaya untuk permintaan yang menggunakan catatan alias untuk merutekan lalu lintas.

Lihat prosedur [Untuk membuat catatan alias Amazon Route 53 untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk](#).

Untuk membuat catatan CNAME untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama zona yang di-hosting yang ingin Anda gunakan untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda.
4. Pilih Buat catatan.
5. Pilih Beralih untuk membuat cepat
6. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke lingkungan Anda, masukkan acme.



Important

Anda tidak dapat membuat data CNAME yang memiliki nama yang sama dengan zona yang di-hosting.

Alias

Jika Anda menggunakan metode pembuatan catatan Pembuatan cepat, aktifkan Alias.

Menilai/Merutekan lalu lintas

Pilih IP address or another value depending on the record type (alamat IP atau nilai lain tergantung jenis catatan) dan masukkan nilai yang Anda dapatkan saat melakukan prosedur di topik [Mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda](#). Jika Anda menggunakan akun yang berbeda untuk membuat zona yang di-hosting Route 53 dan lingkungan Elastic Beanstalk Anda, masukkan atribut CNAME untuk lingkungan Elastic Beanstalk.

Jenis catatan

Pilih CNAME.

TTL (detik)

Terima nilai default 300.

7. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Untuk membuat catatan alias Amazon Route 53 untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama zona yang di-hosting yang ingin Anda gunakan untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda.
4. Pilih Create record (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke lingkungan Anda, masukkan acme.

Menilai/Merutekan lalu lintas

Pilih Alias to Elastic Beanstalk environment (Alias ke lingkungan Elastic Beanstalk), lalu pilih Wilayah tempat titik akhir berasal. Pilih nama domain lingkungan tempat Anda ingin merutekan lalu lintas. Ini adalah nilai yang Anda dapatkan saat Anda melakukan prosedur dalam topik [Mendapatkan nama domain untuk lingkungan Elastic Beanstalk Anda](#).

Jika Anda menggunakan akun yang berbeda untuk membuat zona yang di-hosting Route 53 dan lingkungan Elastic Beanstalk Anda, masukkan atribut CNAME untuk lingkungan Elastic Beanstalk.

Tipe catatan

Terima IPv4 alamat default, A —.

Mengevaluasi kondisi target

Terima nilai default Ya.

6. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Saat propagasi selesai, Anda akan dapat merutekan lalu lintas ke lingkungan Elastic Beanstalk Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Merutekan lalu lintas ke penyeimbang beban ELB

Jika Anda meng-host situs web di beberapa EC2 instans Amazon, Anda dapat mendistribusikan lalu lintas ke situs web Anda di seluruh instans dengan menggunakan penyeimbang beban Elastic Load Balancing (ELB). Layanan ELB secara otomatis menskalakan penyeimbang beban saat lalu lintas ke situs web berubah seiring waktu. Penyeimbang beban juga memantau kondisi target yang terdaftar dan merutekan lalu lintas domain hanya ke target yang sehat.

Untuk rute lalu lintas domain ke penyeimbang beban ELB, gunakan Amazon Route 53 untuk membuat [catatan alias](#) yang menunjuk ke penyeimbang beban Anda. Catatan alias adalah ekstensi Route 53 ke DNS. Ini mirip dengan data CNAME, tetapi Anda dapat membuat data alias untuk domain akar, seperti example.com, dan untuk subdomain, seperti www.example.com. (Anda dapat membuat data CNAME hanya untuk subdomain.)

 Note

Route 53 tidak dikenakan biaya untuk kueri alias ke penyeimbang beban ELB atau lainnya sumber daya AWS .

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- Penyeimbang beban ELB. Anda dapat menggunakan ELB Classic, Application, atau Network Load Balancer. Untuk informasi selengkapnya tentang membuat penyeimbang beban, lihat [Memulai Elastic Load Balancing](#) di Panduan Pengguna Elastic Load Balancing.

Berikan nama untuk penyeimbang beban yang akan membantu Anda mengingat kegunaannya di masa mendatang. Nama yang Anda tentukan saat membuat penyeimbang beban adalah nama yang akan Anda pilih saat membuat catatan alias di konsol Route 53.

- Nama domain terdaftar. Anda dapat menggunakan Route 53 sebagai registrar domain Anda, atau Anda dapat menggunakan registrar lain.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke penyeimbang beban ELB

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke penyeimbang beban ELB, lakukan prosedur berikut.

Untuk merutekan lalu lintas ke penyeimbang beban ELB

1. Jika Anda membuat zona yang di-hosting Route 53 dan penyeimbang beban ELB menggunakan akun yang sama, lewati ke langkah 2.

Jika Anda membuat zona yang di-hosting dan penyeimbang beban ELB menggunakan akun yang berbeda, lakukan prosedur [Mendapatkan nama DNS untuk penyeimbang beban Elastic Load Balancing](#) untuk mendapatkan nama DNS untuk penyeimbang beban.

2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Pada panel navigasi, pilih Zona yang di-hosting.
4. Pilih nama zona yang di-hosting yang memiliki nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke penyeimbang beban Anda.
5. Pilih Create record (Buat catatan).
6. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain atau subdomain yang ingin Anda gunakan untuk merutekan lalu lintas ke penyeimbang beban ELB Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke penyeimbang beban Anda, masukkan acme.

Alias

Jika Anda menggunakan metode pembuatan catatan Pembuatan cepat, aktifkan Alias.

Menilai/Merutekan lalu lintas

Pilih Alias to Application and Classic Load Balancer (Alias ke Aplikasi dan Classic Load Balancer) atau Alias to Network Load Balancer (Alias ke Network Load Balancer), lalu pilih Wilayah tempat titik akhir berasal.

Jika Anda membuat zona yang dihosting dan penyeimbang beban ELB menggunakan AWS akun yang sama, pilih nama DNS yang Anda tetapkan ke penyeimbang beban saat Anda membuatnya.

Jika Anda membuat zona yang dihosting dan penyeimbang beban ELB menggunakan akun yang berbeda, masukkan nilai yang Anda dapatkan di langkah 1 prosedur ini.

 Note

Konsol menambahkan dualstack. ke nama DNS aplikasi dan Classic Load Balancer dari akun AWS yang sama saja. Ketika klien, seperti browser web, meminta alamat IP untuk nama domain Anda (example.com) atau nama subdomain (www.example.com), klien dapat meminta alamat (catatan A), IPv4 alamat (catatan AAAA), atau keduanya IPv4 dan IPv6 IPv6 alamat (dalam permintaan terpisah dengan yang pertama). IPv4 Penunjukan dualstack. memungkinkan Route 53 untuk merespons dengan alamat IP yang sesuai untuk penyeimbang beban Anda berdasarkan format alamat IP yang diminta klien. Anda harus menambahkan dualstack. untuk Aplikasi dan Classic Load Balancer dari akun yang berbeda.

Tipe catatan

Pilih A — IPv4 alamat.

Mengevaluasi Kondisi Target

Jika Anda ingin Route 53 untuk merutekan lalu lintas berdasarkan kesehatan sumber daya Anda, pilih Ya. Untuk informasi selengkapnya tentang memeriksa kondisi sumber daya Anda, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

7. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Saat propagasi selesai, Anda akan dapat merutekan lalu lintas ke penyeimbang beban Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Merutekan lalu lintas ke situs web yang di-host di bucket Amazon S3

Topik ini menyediakan prosedur komprehensif untuk merutekan lalu lintas DNS ke bucket Amazon Simple Storage Service yang dikonfigurasi untuk hosting situs web statis. Jika Anda menyiapkan situs

web statis dengan Amazon Simple Storage Service, lihat [Gunakan domain Anda untuk situs web statis di bucket Amazon S3](#) tutorial lengkapnya.

Amazon Simple Storage Service (Amazon S3), menyediakan [penyimpanan cloud](#) yang aman, tahan lama, dan sangat dapat diskalakan. Anda dapat mengonfigurasi bucket S3 untuk meng-host situs web statis yang dapat menyertakan halaman web dan skrip sisi klien. (S3 tidak mendukung pembuatan skrip sisi server.)

Untuk merutekan lalu lintas domain ke bucket S3, gunakan Amazon Route 53 untuk membuat [catatan Alias](#) yang menunjuk ke bucket Anda. Catatan alias adalah ekstensi Route 53 ke DNS. Ini mirip dengan data CNAME, kecuali Anda dapat membuat data alias untuk domain akar, seperti example.com, dan untuk subdomain, seperti www.example.com. Anda dapat membuat data CNAME hanya untuk subdomain.

Note

Route 53 tidak mengenakan biaya untuk kueri alias ke bucket S3 atau sumber daya AWS lainnya.

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- Bucket S3 yang dikonfigurasi untuk meng-host situs web statis.

Untuk informasi selengkapnya, lihat [Tutorial: Mengonfigurasi situs web statis menggunakan domain khusus yang terdaftar dengan Route 53](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Important

Bucket harus memiliki nama yang sama dengan domain atau subdomain Anda. Misalnya, jika Anda ingin menggunakan subdomain acme.example.com, nama bucket harus acme.example.com.

Anda dapat merutekan lalu lintas untuk domain dan subdomainnya, seperti `example.com` dan `www.example.com`, ke satu bucket. Buat bucket untuk domain dan setiap subdomain, dan konfigurasi semua kecuali satu bucket untuk mengalihkan lalu lintas ke bucket yang tersisa.

 Note

Bucket S3 yang dikonfigurasi sebagai titik akhir situs web tidak mendukung SSL/TLS, jadi Anda perlu merutekan lalu lintas ke CloudFront distribusi dan menggunakan bucket S3 sebagai asal distribusi.

Untuk petunjuk tentang cara membuat CloudFront distribusi, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#).

- Nama domain terdaftar. Anda dapat menggunakan Route 53 sebagai registrar domain Anda, atau Anda dapat menggunakan registrar lain.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke Bucket S3

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke bucket S3 yang dikonfigurasi untuk meng-host situs web statis, lakukan prosedur berikut.

Untuk merutekan lalu lintas ke bucket S3

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama zona yang di-hosting yang memiliki nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke bucket S3 Anda.
4. Pilih Create record (Buat catatan).
5. Tentukan nilai-nilai berikut ini:

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke bucket S3 Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk merutekan lalu lintas ke bucket Anda, masukkan acme.

Tipe catatan

Pilih A — IPv4 alamat.

Alias

Nyalakan Alias.

Rute lalu lintas ke

Pilih Alias to S3 website endpoint (Alias ke titik akhir situs web S3), lalu pilih Wilayah tempat titik akhir berasal.

Pilih bucket yang memiliki nama yang sama yang Anda tentukan untuk Nama catatan.

Daftar ini akan menyertakan bucket hanya jika bucket memenuhi persyaratan berikut:

- Nama bucket sama dengan nama catatan yang Anda buat.
- Bucket dikonfigurasi sebagai titik akhir situs web.
- Bucket dibuat oleh akun AWS saat ini.

Jika Anda membuat bucket menggunakan akun AWS yang berbeda, masukkan nama Wilayah yang Anda buat di bucket S3. Untuk format yang benar untuk nama Wilayah, lihat kolom titik akhir Situs web di tabel titik akhir [situs Amazon S3](#) di. Referensi Umum Amazon Web Services

Mengevaluasi Kondisi Target

Pilih No. Untuk informasi tentang mengevaluasi kesehatan target, lihat [Mengevaluasi Kondisi Target](#).

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

6. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Saat propagasi selesai, Anda akan dapat merutekan lalu lintas ke bucket S3 Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Merutekan lalu lintas ke titik akhir antarmuka Amazon Virtual Private Cloud dengan menggunakan nama domain Anda

Anda dapat menggunakan AWS PrivateLink untuk mengakses layanan yang dipilih dengan titik akhir antarmuka Amazon Virtual Private Cloud (Amazon VPC). Layanan ini mencakup beberapa AWS layanan, layanan yang diselenggarakan oleh AWS pelanggan lain dan mitra mereka sendiri VPCs, dan layanan AWS Marketplace mitra yang didukung.

Untuk merutekan lalu lintas domain ke titik akhir antarmuka, menggunakan Amazon Route 53 untuk membuat catatan alias. Catatan alias adalah ekstensi Route 53 ke DNS. Ini mirip dengan data CNAME, tetapi Anda dapat membuat data alias untuk domain akar, seperti `example.com`, dan untuk subdomain, seperti `www.example.com`. Anda dapat membuat data CNAME hanya untuk subdomain.

Note

Route 53 tidak mengenakan biaya untuk kueri alias ke titik akhir antarmuka atau sumber daya lainnya. AWS

Topik

- [Prasyarat](#)
- [Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir antarmuka VPC Amazon](#)

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

- Titik akhir antarmuka Amazon VPC. Untuk informasi selengkapnya, lihat [Antarmuka VPC endpoint \(AWS PrivateLink\)](#) dalam Panduan Pengguna Amazon VPC.

- Nama domain terdaftar. Anda dapat menggunakan Amazon Route 53 sebagai registrar domain Anda, atau Anda dapat menggunakan registrar yang berbeda.
- Route 53 sebagai layanan DNS untuk domain. Jika Anda mendaftarkan nama domain Anda dengan menggunakan Route 53, kami secara otomatis mengonfigurasi Route 53 sebagai layanan DNS untuk domain.

Untuk informasi tentang cara menggunakan Route 53 sebagai penyedia layanan DNS untuk domain Anda, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir antarmuka VPC Amazon

Untuk mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir antarmuka VPC Amazon, lakukan prosedur berikut.

Untuk merutekan lalu lintas ke titik akhir antarmuka Amazon VPC

1. Jika Anda membuat zona yang di-hosting Route 53 dan titik akhir antarmuka Amazon VPC menggunakan akun yang sama, lewati ke langkah 2.

Jika Anda membuat zona yang di-hosting dan titik akhir antarmuka menggunakan akun yang berbeda, dapatkan nama layanan untuk titik akhir antarmuka:

- a. Masuk ke Konsol Manajemen AWS dan buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
 - b. Di panel navigasi, pilih Titik Akhir.
 - c. Di panel kanan, pilih titik akhir yang ingin Anda rutekan lalu lintas internetnya.
 - d. Di panel bawah, dapatkan nilai nama DNS, misalnya, `vpce-0fd00dd593 example-example.cloudtrail.us-west-2.vpce.amazonaws.com`.
2. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 3. Pada panel navigasi, pilih Zona yang di-hosting.
 4. Pilih nama zona yang di-hosting yang memiliki nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke titik akhir antarmuka Anda.
 5. Pilih Create record (Buat catatan).
 6. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke titik akhir antarmuka Amazon VPC Anda.

Alias

Jika Anda menggunakan metode pembuatan catatan Pembuatan cepat, aktifkan Alias.

Menilai/Merutekan lalu lintas

Pilih Alias to VPC endpoint (Alias ke VPC endpoint), lalu pilih Wilayah tempat titik akhir berasal.

Cara Anda menentukan nilai untuk Titik Akhir tergantung pada apakah Anda membuat zona yang dihosting dan titik akhir antarmuka menggunakan AWS akun yang sama atau akun yang berbeda:

- Akun yang sama – Pilih daftar, dan temukan kategori Amazon VPC endpoints (Titik akhir Amazon VPC). Kemudian pilih nama DNS dari titik akhir antarmuka yang ingin Anda rutekan lalu lintas internetnya.
- Akun yang berbeda – Masukkan nilai yang Anda dapatkan pada langkah 1 dari prosedur ini.

Tipe catatan

Pilih A — IPv4 alamat.

Mengevaluasi Kondisi Target

Pilih No. Untuk informasi tentang mengevaluasi kesehatan target, lihat [Mengevaluasi Kondisi Target](#).

7. Pilih Create records (Buat catatan).

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Saat propagasi selesai, Anda akan dapat merutekan lalu lintas ke titik akhir antarmuka Anda dengan menggunakan nama catatan alias yang Anda buat dalam prosedur ini.

Merutekan lalu lintas ke Amazon WorkMail

Anda dapat menggunakan Route 53 untuk merutekan lalu lintas ke domain WorkMail email Amazon Anda. Nama zona host Route 53 Anda (seperti example.com) harus cocok dengan nama domain Amazon WorkMail .

Note

Anda dapat merutekan lalu lintas ke WorkMail domain Amazon hanya untuk zona yang dihosting publik.

Untuk merutekan lalu lintas ke Amazon WorkMail, lakukan empat prosedur berikut.

Untuk mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda dan menambahkan WorkMail organisasi Amazon dan domain email

1. Jika Anda belum mendaftarkan nama domain yang ingin Anda gunakan di alamat email Anda (seperti john@example.com), daftarkan domain sekarang agar Anda tahu bahwa domain tersebut tersedia. Untuk informasi selengkapnya, lihat [Mendaftarkan domain baru](#).

Jika Amazon Route 53 bukan layanan DNS untuk domain email yang Anda tambahkan ke Amazon WorkMail, migrasi layanan DNS untuk domain tersebut ke Route 53. Untuk informasi selengkapnya, lihat [Membuat Amazon Route 53 menjadi layanan DNS untuk domain yang ada](#).

2. Tambahkan WorkMail organisasi Amazon dan domain email. Untuk informasi selengkapnya, lihat [Memulai pengguna baru](#) di Panduan WorkMail Administrator Amazon.

Untuk membuat catatan Route 53 TXT untuk Amazon WorkMail

1. Di panel navigasi WorkMail konsol Amazon, pilih Domain.
2. Pilih nama domain email, seperti example.com yang ingin Anda gunakan untuk merutekan lalu lintas ke Amazon. WorkMail
3. Buka tab peramban lain, dan buka [Konsol Route 53](#).
4. Di konsol Route 53, lakukan hal berikut:
 - a. Pada panel navigasi, pilih Zona yang di-hosting.

- b. Pilih nama zona yang dihosting yang ingin Anda gunakan untuk domain WorkMail email Amazon Anda.
5. Di WorkMail konsol Amazon, di bagian Langkah 1: Verifikasi kepemilikan domain, buka kolom Hostname, dan salin bagian nilai yang mendahului nama domain email Anda.

Misalnya, jika domain WorkMail email Amazon Anda adalah example.com dan nilai Hostname adalah _amazonses.example.com, salin _amazonses.
6. Di konsol Route 53, lakukan hal berikut:
 - a. Pilih Create record (Buat catatan), dan pilih Simple routing (Perutean sederhana).
 - b. Untuk Nama catatan, sisipkan nilai yang Anda salin dalam langkah 5.
 - c. Untuk Record type (Jenis catatan), pilih TXT – Text (TXT - Teks).
7. Di WorkMail konsol Amazon, untuk catatan TXT, salin nilai kolom Nilai, termasuk tanda kutip.
8. Di konsol Route 53, lakukan hal berikut:
 - a. Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas) Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan), dan tempel nilai yang Anda salin dalam langkah 7.

Jangan mengubah pengaturan lainnya.
 - b. Pilih Create (Buat).

Untuk membuat catatan Route 53 MX untuk Amazon WorkMail

1. Di WorkMail konsol Amazon, di bagian Langkah 2: Selesaikan pengaturan domain, buka baris yang memiliki tipe Rekam MX, dan salin nilai kolom Nilai.
2. Di konsol Route 53, lakukan hal berikut:
 - a. Pilih Buat catatan.
 - b. Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan), dan tempel nilai yang Anda salin dalam langkah 1.
 - c. Untuk Record type (Jenis catatan), pilih MX – Mail Exchange.

Jangan mengubah pengaturan lainnya.
 - d. Pilih Create records (Buat catatan).

Untuk membuat empat catatan Route 53 CNAME untuk Amazon WorkMail

1. Di WorkMail konsol Amazon, di bagian Langkah 2: Selesaikan pengaturan domain, buka baris pertama yang memiliki tipe Rekam CNAME. Di kolom Hostname, salin bagian nilai yang mendahului nama domain email Anda.

Misalnya, jika domain WorkMail email Amazon Anda adalah example.com dan nilai Hostname adalah autodiscover.example.com, salin autodiscover.

2. Di konsol Route 53, lakukan hal berikut:
 - a. Pilih Buat catatan.
 - b. Untuk Nama catatan, tempel nilai yang Anda salin dalam langkah 1.
 - c. Untuk Record type (Jenis catatan), pilih CNAME – Canonical Name (CNAME – Nama Kanonis).
3. Di WorkMail konsol Amazon, di baris pertama yang memiliki tipe Rekam CNAME, salin nilai kolom Nilai.
4. Di konsol Route 53, lakukan hal berikut:
 - a. Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), Pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan), dan tempel nilai yang Anda salin dalam langkah 3.

Jangan mengubah pengaturan lainnya.
 - b. Pilih Create records (Buat catatan).
5. Ulangi langkah 1 hingga 4 untuk catatan CNAME yang tersisa yang terdaftar di WorkMail konsol Amazon.

Merutekan lalu lintas ke titik akhir domain OpenSearch Layanan Amazon

Amazon OpenSearch Service adalah layanan terkelola yang memudahkan penerapan, pengoperasian, dan skala OpenSearch cluster di. AWS Cloud Domain OpenSearch Layanan Layanan identik dengan kluster OpenSearch Layanan. Domain adalah klaster dengan pengaturan, tipe instans, jumlah instans, dan sumber daya penyimpanan yang Anda tentukan. Untuk informasi selengkapnya, lihat [Apa itu OpenSearch Layanan Amazon](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

Domain OpenSearch Layanan yang memiliki nama domain khusus, seperti `example.com` yang cocok dengan nama catatan Route 53 yang ingin Anda buat.

Untuk informasi selengkapnya, lihat topik berikut:

- [Memulai](#) di Panduan Pengembang OpenSearch Layanan Amazon.
- [Membuat titik akhir kustom](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir domain OpenSearch Layanan Amazon

Untuk menggunakan Route 53 untuk merutekan lalu lintas ke OpenSearch Layanan, pertama-tama Anda mendapatkan titik akhir domain yang disediakan oleh OpenSearch Layanan. Titik akhir tumpukan ganda ini disediakan hanya jika titik akhir kustom diaktifkan pada domain OpenSearch Layanan dengan mode jaringan tumpukan ganda. Untuk informasi selengkapnya, lihat [Membuat titik akhir kustom](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Untuk merutekan lalu lintas ke OpenSearch titik akhir Layanan

1. Buka <https://aws.amazon.com> dan pilih Masuk ke Konsol.
2. Di bawah Analytics, pilih OpenSearch Layanan Amazon.
3. Di bawah Kluster terkelola pilih Domain.
4. Pada halaman Domain pilih nama domain yang ingin Anda rutekan lalu lintas.
5. Pada halaman detail domain salin nilai untuk titik akhir Domain v2 (tumpukan ganda).
6. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
7. Pada panel navigasi, pilih Zona yang di-hosting.
8. Pilih nama yang ditautkan dari zona yang dihosting untuk domain yang ingin Anda gunakan untuk merutekan lalu lintas ke titik akhir OpenSearch Layanan Anda. Nama domain harus sesuai dengan titik akhir kustom yang ditentukan dalam OpenSearch Layanan.
9. Pilih Buat catatan.

Anda dapat menggunakan wizard untuk membuat catatan atau memilih Beralih untuk membuat cepat.

10. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke titik akhir domain OpenSearch Layanan Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk mengarahkan lalu lintas ke distribusi Anda, masukkan acme.

Alias

Jika Anda menggunakan metode pembuatan catatan Pembuatan cepat, aktifkan Alias.

Nilai/Rutekan lalu lintas ke

Pilih titik akhir domain Alias ke OpenSearch Layanan. Pilih Wilayah tempat domain OpenSearch Layanan dibuat, dan pilih nilai yang Anda dapatkan di langkah 5.

Tipe catatan

Pilih alamat A — IPv4 alamat, AAAA — IPv6 atau keduanya untuk dual-stack.

Mengevaluasi Kondisi Target

Pilih No. Untuk informasi tentang mengevaluasi kesehatan target, lihat [Mengevaluasi Kondisi Target](#).

11. Pilih Create records (Buat catatan).

Merutekan lalu lintas ke titik akhir domain layanan Amazon VPC Lattice

Amazon VPC Lattice adalah layanan jaringan aplikasi terkelola penuh yang Anda gunakan untuk menghubungkan, mengamankan, dan memantau layanan dan sumber daya untuk aplikasi Anda. Anda dapat menggunakan VPC Lattice dengan satu virtual private cloud (VPC) atau beberapa VPCs dari satu akun atau lebih. Untuk informasi selengkapnya, lihat [Apa itu Amazon VPC Lattice di Panduan Pengguna Amazon VPC Lattice](#).

Prasyarat

Untuk memulai, Anda memerlukan yang berikut ini:

Domain layanan VPC Lattice yang memiliki nama domain khusus, seperti `example.com` yang cocok dengan nama catatan Route 53 yang ingin Anda buat.

Untuk informasi selengkapnya, lihat [Mengaitkan nama domain khusus dengan layanan Anda](#) di Panduan Pengguna Amazon VPC Lattice.

Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke titik akhir domain layanan VPC Lattice

Untuk menggunakan Route 53 untuk merutekan lalu lintas ke domain layanan Amazon VPC Lattice, Anda terlebih dahulu mendapatkan endpoint layanan domain yang disediakan oleh VPC Lattice.

Untuk informasi selengkapnya, lihat [Mengaitkan nama domain khusus dengan layanan Anda](#) di Panduan Pengguna Amazon VPC Lattice.

Untuk merutekan lalu lintas ke titik akhir domain layanan VPC Lattice

1. Buka <https://aws.amazon.com> dan pilih Masuk ke Konsol.
2. Di bawah Networking & Content Delivery, pilih VPC.
3. Di bawah PrivateLink dan Kisi pilih Layanan Kisi.
4. Buat layanan VPC Lattice atau pilih layanan VPC Lattice yang ada.

Note

Saat membuat layanan VPC Lattice, Anda harus menentukan konfigurasi domain kustom dan menyediakan nama domain khusus. Jika Anda memilih layanan yang ada, itu juga harus memiliki domain khusus.

5. Di bawah konfigurasi Domain, salin nilai untuk nama domain kustom.
6. Buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
7. Pada panel navigasi, pilih Zona yang di-hosting.
8. Pilih nama yang ditautkan dari zona yang dihosting untuk domain yang ingin Anda gunakan untuk merutekan lalu lintas ke titik akhir domain layanan VPC Lattice Anda. Nama domain harus sesuai dengan titik akhir domain kustom yang ditentukan dalam VPC Lattice.
9. Pilih Buat catatan.

Anda dapat menggunakan wizard untuk membuat catatan atau memilih Beralih untuk membuat cepat.

10. Tentukan nilai-nilai berikut ini:

Kebijakan perutean

Pilih kebijakan perutean yang sesuai. Untuk informasi selengkapnya, lihat [Memilih kebijakan perutean](#).

Nama catatan

Masukkan nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke titik akhir domain layanan VPC Lattice Anda. Nilai default adalah nama zona yang di-hosting.

Misalnya, jika nama zona yang di-hosting adalah example.com dan Anda ingin menggunakan acme.example.com untuk mengarahkan lalu lintas ke distribusi Anda, masukkan acme.

Alias

Jika Anda menggunakan metode pembuatan catatan Pembuatan cepat, aktifkan Alias.

Nilai/Rutekan lalu lintas ke

Pilih layanan Alias ke VPC Lattice. Pilih Wilayah tempat domain layanan VPC Lattice dibuat, dan pilih nilai yang Anda dapatkan di langkah 5.

Tipe catatan

Pilih alamat A — IPv4 alamat, AAAA — IPv6 alamat, atau keduanya untuk dual-stack.

Mengevaluasi Kondisi Target

Pilih No. Untuk informasi tentang mengevaluasi kesehatan target, lihat [Mengevaluasi Kondisi Target](#).

11. Pilih Create records (Buat catatan).

Merutekan lalu lintas ke sumber daya lain AWS

Berikut ini adalah daftar topik dalam panduan lain tentang cara menggunakan Route 53 untuk mengarahkan lalu lintas ke layanan tersebut.

- [Menggunakan AWS Cloud Map](#) dalam Panduan AWS Cloud Map Pengguna.

- [Mengelola domain kustom](#) di Panduan AWS App Runner Pengembang.
- [Menggunakan Route 53 sebagai penyedia DNS](#) di Panduan AWS Transfer Family Pengguna.
- [Menggunakan Route 53 untuk mengarahkan domain ke instans Amazon Lightsail](#).

Membuat pemeriksaan kesehatan Amazon Route 53

Pemeriksaan kondisi Amazon Route 53 memantau kondisi dan performa aplikasi web, server web, dan sumber daya lainnya. Setiap pemeriksaan kondisi yang Anda buat dapat memantau hal berikut:

- Kesehatan sumber daya yang ditentukan, seperti server web.
- Status pemeriksaan kondisi lainnya.
- Status CloudWatch alarm Amazon.
- Selain itu, dengan Amazon Application Recovery Controller (ARC), Anda dapat mengatur pemeriksaan kesehatan kontrol perutean dengan catatan failover DNS untuk mengelola failover lalu lintas untuk aplikasi Anda. Untuk mempelajari selengkapnya, lihat [Panduan Pengembang Amazon Application Recovery Controller \(ARC\)](#).

Untuk gambaran umum jenis pemeriksaan kondisi, lihat [Jenis pemeriksaan kondisi Amazon Route 53](#). Untuk informasi tentang membuat pemeriksaan kondisi, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Setelah membuat pemeriksaan kondisi, Anda bisa mendapatkan status pemeriksaan kondisi, mendapatkan notifikasi saat status berubah, dan mengonfigurasi failover DNS:

Mendapatkan status dan notifikasi pemeriksaan kondisi

Anda dapat melihat status pemeriksaan kondisi saat ini dan terbaru di konsol Route 53. Anda juga dapat bekerja dengan pemeriksaan kesehatan secara terprogram melalui salah satu AWS SDKs, API AWS Command Line Interface AWS Tools for Windows PowerShell, atau Route 53.

Jika Anda ingin menerima pemberitahuan ketika status pemeriksaan kesehatan berubah, Anda dapat mengonfigurasi CloudWatch alarm Amazon untuk setiap pemeriksaan kesehatan.

Untuk informasi tentang melihat status pemeriksaan kondisi dan menerima notifikasi, lihat [Memantau status pemeriksaan kondisi dan mendapatkan notifikasi](#).

Mengonfigurasi failover DNS

Jika Anda memiliki beberapa sumber daya yang menjalankan fungsi yang sama, Anda dapat mengonfigurasi failover DNS sehingga Route 53 akan merutekan lalu lintas Anda dari sumber daya yang tidak sehat ke sumber daya yang sehat. Misalnya, jika Anda memiliki dua server web dan satu server web menjadi tidak sehat, Route 53 dapat merutekan lalu lintas ke server web lainnya. Untuk informasi selengkapnya, lihat [Mengonfigurasi failover DNS](#).

Topik

- [Jenis pemeriksaan kondisi Amazon Route 53](#)
- [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#)
- [Membuat, memperbarui, dan menghapus pemeriksaan kondisi](#)
- [Mengonfigurasi failover DNS](#)
- [Penamaan dan penandaan pemeriksaan kondisi](#)
- [Menggunakan pemeriksaan kondisi dengan versi API Amazon Route 53 yang lebih awal dari 2012-12-12](#)

Jenis pemeriksaan kondisi Amazon Route 53

Anda dapat membuat jenis pemeriksaan kondisi Amazon Route 53 berikut:

Pemeriksaan kondisi yang memantau titik akhir

Anda dapat mengonfigurasi pemeriksaan kondisi yang memantau titik akhir yang Anda tentukan dengan alamat IP atau nama domain. Pada interval reguler yang Anda tentukan, Route 53 mengirimkan permintaan otomatis melalui internet ke aplikasi, server, atau sumber daya lain untuk memverifikasi bahwa semuanya dapat dijangkau, tersedia, dan fungsional. Secara opsional, Anda dapat mengonfigurasi pemeriksaan kondisi untuk membuat permintaan yang serupa dengan permintaan yang dibuat pengguna Anda, seperti meminta halaman web dari URL tertentu.

Pemeriksaan kondisi yang memantau pemeriksaan kondisi lainnya (pemeriksaan kondisi yang dihitung)

Anda dapat membuat pemeriksaan kondisi yang memantau apakah Route 53 menganggap pemeriksaan kondisi lainnya sehat atau tidak sehat. Situasi di mana tindakan ini mungkin berguna adalah ketika Anda memiliki beberapa sumber daya yang melakukan fungsi yang sama, seperti beberapa server web, dan kekhawatiran utama Anda adalah apakah sejumlah minimum sumber daya dalam kondisi sehat. Anda dapat membuat pemeriksaan kondisi untuk setiap sumber daya tanpa mengonfigurasi notifikasi untuk pemeriksaan kondisi tersebut. Kemudian Anda dapat membuat pemeriksaan kondisi yang memantau status pemeriksaan kondisi lainnya dan yang memberitahu Anda hanya ketika jumlah sumber daya web yang tersedia turun di bawah ambang batas yang ditentukan.

Pemeriksaan Kesehatan yang Memantau CloudWatch Alarm

Anda dapat membuat CloudWatch alarm yang memantau status CloudWatch metrik, seperti jumlah peristiwa baca terbatas untuk database Amazon DynamoDB atau jumlah host Elastic Load Balancing yang dianggap sehat. Setelah Anda membuat alarm, Anda dapat membuat pemeriksaan kesehatan yang memantau aliran data yang sama yang CloudWatch memantau alarm.

Untuk meningkatkan ketahanan dan ketersediaan, Route 53 tidak menunggu CloudWatch alarm masuk ke negara bagian ALARM. Status pemeriksaan kesehatan berubah dari sehat menjadi tidak sehat berdasarkan aliran data dan kriteria dalam CloudWatch alarm.

Route 53 mendukung CloudWatch alarm dengan fitur-fitur berikut:

- Metrik resolusi standar. Metrik resolusi tinggi tidak didukung. Untuk informasi selengkapnya, lihat [Metrik resolusi tinggi](#) di CloudWatch Panduan Pengguna Amazon.
- Statistik: Rata-rata, Minimum, Maksimum, Jumlah, dan SampleCount. Perpanjangan statistik tidak didukung.
- Route 53 tidak mendukung alarm “M out of N”. Untuk informasi selengkapnya, lihat [Mengevaluasi alarm](#) di CloudWatch panduan Amazon.
- Pemeriksaan kesehatan hanya dapat memantau CloudWatch alarm yang ada di AWS akun yang sama dengan pemeriksaan kesehatan.
- Route 53 tidak mendukung alarm yang menggunakan [matematika metrik](#) untuk menanyakan beberapa CloudWatch metrik.

Pengontrol perutean Amazon Application Recovery Controller (ARC)

Pemeriksaan kesehatan di ARC dikaitkan dengan kontrol perutean, yang merupakan sakelar on/off sederhana. Anda mengonfigurasi setiap pemeriksaan kondisi kontrol perutean dengan catatan DNS failover. Kemudian Anda cukup memperbarui kontrol perutean Anda di ARC untuk mengalihkan lalu lintas dan gagal atas aplikasi Anda, misalnya, di Availability Zones atau -Regions. AWS Untuk informasi selengkapnya, lihat [Kontrol perutean di ARC](#) di panduan pengembang ARC.

Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat

Metode yang digunakan Amazon Route 53 untuk menentukan apakah pemeriksaan kondisi sehat tergantung pada jenis pemeriksaan kondisi.

Bagaimana Route 53 menentukan status pemeriksaan kondisi yang memantau titik akhir

Route 53 memiliki pemeriksa kondisi di banyak lokasi di seluruh dunia. Ketika Anda membuat pemeriksaan kondisi yang memantau titik akhir, pemeriksa kondisi mulai mengirim permintaan ke titik akhir yang Anda tentukan untuk menentukan apakah titik akhir sehat. Anda dapat memilih lokasi mana yang ingin digunakan Route 53, dan Anda dapat menentukan interval antara pemeriksaan: setiap 10 detik atau setiap 30 detik. Perhatikan bahwa pemeriksa kondisi Route 53 di pusat data yang berbeda tidak berkoordinasi satu sama lain, sehingga terkadang Anda akan melihat beberapa permintaan per detik terlepas dari interval yang dipilih, diikuti beberapa detik tanpa pemeriksaan kondisi sama sekali.

Setiap pemeriksa kondisi mengevaluasi kondisi titik akhir berdasarkan dua nilai:

- Waktu respons. Sumber daya dapat lambat merespons atau gagal merespons permintaan pemeriksaan kondisi karena berbagai alasan. Misalnya, sumber daya dimatikan untuk pemeliharaan, berada di bawah serangan penolakan layanan (DDoS) terdistribusi, atau jaringan mati.
- Apakah titik akhir merespons sejumlah pemeriksaan kondisi berturut-turut yang Anda tentukan (ambang batas kegagalan)

Route 53 mengagregat data dari pemeriksa kondisi dan menentukan apakah titik akhir sehat:

- Jika lebih dari 18% pemeriksa kondisi melaporkan bahwa titik akhir sehat, Route 53 menganggapnya sehat.
- Jika 18% atau kurang pemeriksa kondisi melaporkan bahwa titik akhir sehat, Route 53 menganggapnya tidak sehat.

Nilai 18% dipilih untuk memastikan bahwa pemeriksa kondisi di beberapa wilayah menganggap titik akhir sehat. Hal ini mencegah agar titik akhir dianggap tidak sehat hanya karena syarat jaringan telah

mengisolasi titik akhir dari beberapa lokasi pemeriksaan kondisi. Nilai ini mungkin berubah di rilis di masa mendatang.

Waktu respons yang digunakan pemeriksaan kondisi individu untuk menentukan apakah titik akhir sehat tergantung pada jenis pemeriksaan kondisi:

- Pemeriksaan kondisi HTTP dan HTTPS – Route 53 harus mampu membuat koneksi TCP dengan titik akhir dalam waktu empat detik. Selain itu, titik akhir harus merespons dengan kode status HTTP 2xx atau 3xx dalam waktu dua detik setelah menghubungkan.

 Note

Pemeriksaan kesehatan HTTPS tidak memvalidasi SSL/TLS sertifikat, jadi pemeriksaan tidak gagal jika sertifikat tidak valid atau kedaluwarsa.

- Pemeriksaan kondisi TCP – Route 53 harus mampu membuat koneksi TCP dengan titik akhir dalam waktu sepuluh detik.
- Pemeriksaan kondisi HTTP dan HTTPS dengan pencocokan string – Seperti pemeriksaan kondisi HTTP dan HTTPS, Route 53 harus mampu membuat koneksi TCP dengan titik akhir dalam waktu empat detik, dan titik akhir harus merespons dengan kode status HTTP 2xx atau 3xx dalam waktu dua detik setelah menghubungkan.

Setelah menerima kode status HTTP, pemeriksaan kondisi Route 53 harus menerima respons isi dari titik akhir dalam dua detik berikutnya. Route 53 mencari isi respons untuk string yang Anda tentukan. Seluruh string harus muncul dalam 5.120 byte pertama pada isi respons atau pemeriksaan kondisi titik akhir akan gagal. Jika menggunakan konsol Route 53, Anda menentukan string di bidang Cari String. Jika menggunakan API Route 53, Anda menentukan string dalam elemen `SearchString` ketika membuat pemeriksaan kondisi.

Untuk pemeriksaan kesehatan yang memantau titik akhir (kecuali pemeriksaan kesehatan TCP), jika respons dari titik akhir menyertakan header apa pun, header harus dalam format yang ditentukan dalam RFC7230, Protokol Transfer Hypertext (HTTP/1.1): Sintaks Pesan dan Perutean, bagian 3.2, “Bidang Header.”

Route 53 menganggap pemeriksaan kondisi baru dalam kondisi sehat hingga ada cukup data untuk menentukan status yang sebenarnya, sehat atau tidak sehat. Jika Anda memilih opsi untuk membalikkan status pemeriksaan kondisi, Route 53 menganggap pemeriksaan kondisi baru tidak sehat hingga ada cukup data.

Bagaimana Route 53 menentukan status pemeriksaan kondisi yang memantau pemeriksaan kondisi lain

Pemeriksaan kondisi dapat memantau status pemeriksaan kondisi lainnya; pemeriksaan kondisi jenis ini dikenal sebagai pemeriksaan kondisi yang dihitung. Pemeriksaan kondisi yang melakukan pemantauan adalah pemeriksaan kondisi induk, dan pemeriksaan kondisi yang dipantau adalah pemeriksaan kondisi anak. Satu pemeriksaan kondisi induk dapat memantau hingga 255 pemeriksaan kondisi anak. Berikut adalah cara kerja pemantauan:

- Route 53 menambahkan jumlah pemeriksaan kondisi anak yang dianggap sehat.
- Route 53 membandingkan angka tersebut dengan jumlah pemeriksaan kondisi anak yang harus sehat agar status pemeriksaan kondisi induk dianggap sehat.

Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kondisi lainnya \(pemeriksaan kondisi yang dihitung\)](#) di [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#).

Route 53 menganggap pemeriksaan kondisi baru dalam kondisi sehat hingga ada cukup data untuk menentukan status yang sebenarnya, sehat atau tidak sehat. Jika Anda memilih opsi untuk membalikkan status pemeriksaan kondisi, Route 53 menganggap pemeriksaan kondisi baru tidak sehat hingga ada cukup data.

Bagaimana Route 53 menentukan status pemeriksaan kesehatan yang memantau CloudWatch alarm

Saat Anda membuat pemeriksaan kesehatan yang didasarkan pada CloudWatch alarm, Route 53 memantau aliran data untuk alarm yang sesuai alih-alih memantau status alarm. Jika aliran data menunjukkan bahwa alarm dalam status OKE, pemeriksaan kondisi dianggap sehat. Jika aliran data menunjukkan bahwa alarm dalam status Alarm, pemeriksaan kondisi dianggap tidak sehat. Jika aliran data tidak memberikan informasi yang cukup untuk menentukan status alarm, status pemeriksaan kondisi tergantung pada pengaturan untuk Status pemeriksaan kondisi: sehat, tidak sehat, atau status terakhir. (Dalam API Route 53, pengaturannya adalah `InsufficientDataHealthStatus`.)

Route 53 tidak mendukung alarm lintas akun CloudWatch .

 Note

Karena pemeriksaan kesehatan Route 53 memantau aliran CloudWatch data alih-alih status CloudWatch alarm, Anda tidak dapat memaksa status pemeriksaan kesehatan berubah dengan menggunakan operasi CloudWatch [SetAlarmState](#) API.

Route 53 menganggap pemeriksaan kondisi baru dalam kondisi sehat hingga ada cukup data untuk menentukan status yang sebenarnya, sehat atau tidak sehat. Jika Anda memilih opsi untuk membalikkan status pemeriksaan kondisi, Route 53 menganggap pemeriksaan kondisi baru tidak sehat hingga ada cukup data.

Membuat, memperbarui, dan menghapus pemeriksaan kondisi

 Important

Jika Anda memperbarui atau menghapus pemeriksaan kondisi yang terkait dengan catatan, tinjau tugas di [Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi](#) sebelum Anda melanjutkan.

Bagian ini mencakup topik-topik berikut yang terkait dengan pengelolaan pemeriksaan kesehatan Route 53:

1. Membuat dan memperbarui pemeriksaan kesehatan:

- Pelajari cara membuat dan memperbarui pemeriksaan kesehatan menggunakan konsol Route 53.
- Pahami nilai yang perlu Anda tentukan saat membuat atau memperbarui pemeriksaan kesehatan, seperti pemantauan titik akhir, protokol, alamat IP, nama domain, dan opsi konfigurasi lanjutan.

2. Nilai yang ditampilkan saat membuat pemeriksaan kesehatan:

- Temukan nilai yang ditampilkan konsol Route 53 berdasarkan masukan Anda saat membuat pemeriksaan kesehatan, seperti URL lengkap atau alamat IP dan port.

3. Memperbarui pemeriksaan kesehatan untuk perubahan CloudWatch alarm:

- Cari tahu cara memperbarui pemeriksaan kesehatan saat Anda mengubah pengaturan CloudWatch alarm terkait.

4. Menghapus pemeriksaan kesehatan:

- Ikuti prosedur untuk menghapus pemeriksaan kesehatan dengan menggunakan konsol Route 53.

5. Memperbarui atau menghapus pemeriksaan kesehatan saat failover DNS dikonfigurasi:

- Pelajari tugas yang disarankan untuk dilakukan saat memperbarui atau menghapus pemeriksaan kesehatan yang terkait dengan catatan DNS untuk memastikan konfigurasi routing dan failover yang tepat.

6. Mengkonfigurasi aturan router dan firewall:

- Pahami cara mengonfigurasi aturan router dan firewall Anda untuk memungkinkan lalu lintas masuk dari pemeriksa kesehatan Route 53, memastikan pemeriksaan kesehatan yang berhasil.

Dengan mengikuti informasi yang disediakan di bagian ini, Anda dapat secara efektif membuat, memperbarui, dan menghapus pemeriksaan kesehatan Route 53, mengelola konfigurasinya, dan memastikan integrasi yang tepat dengan kebijakan failover dan perutean DNS.

Topik

- [Membuat dan memperbarui pemeriksaan kondisi](#)
- [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#)
- [Nilai yang ditampilkan Amazon Route 53 ketika Anda membuat pemeriksaan kondisi](#)
- [Memperbarui pemeriksaan kesehatan saat Anda mengubah pengaturan CloudWatch alarm \(pemeriksaan kesehatan yang hanya memantau CloudWatch alarm\)](#)
- [Menonaktifkan atau mengaktifkan pemeriksaan kesehatan](#)
- [Membalikkan pemeriksaan kesehatan](#)
- [Menghapus pemeriksaan kondisi](#)
- [Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi](#)
- [Mengonfigurasi aturan router dan firewall untuk pemeriksaan kondisi Amazon Route 53](#)

Membuat dan memperbarui pemeriksaan kondisi

Prosedur berikut menjelaskan cara membuat dan memperbarui pemeriksaan kondisi menggunakan konsol Route 53.

 Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk membuat atau memperbarui pemeriksaan kesehatan

1. Jika Anda memperbarui pemeriksaan kondisi yang telah dikaitkan dengan catatan, lakukan tugas yang disarankan di [Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi](#).
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Pemeriksaan Kondisi.
4. Jika Anda ingin memperbarui pemeriksaan kesehatan yang ada, pilih ID yang ditautkan dari pemeriksaan kesehatan, lalu pilih Edit.

Jika Anda ingin membuat pemeriksaan kesehatan, pilih Buat pemeriksaan kesehatan.

5. Masukkan nilai yang berlaku. Perhatikan bahwa beberapa nilai tidak dapat diubah setelah Anda membuat pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#).
6. Pilih Buat pemeriksaan kondisi.

 Note

Route 53 menganggap pemeriksaan kondisi baru dalam kondisi sehat hingga ada cukup data untuk menentukan status yang sebenarnya, sehat atau tidak sehat.

7. Kaitkan pemeriksaan kondisi dengan satu atau beberapa catatan Route 53. Untuk informasi tentang membuat dan memperbarui catatan, lihat [Bekerja dengan catatan](#).

Old console

Untuk membuat atau memperbarui pemeriksaan kesehatan

1. Jika Anda memperbarui pemeriksaan kondisi yang telah dikaitkan dengan catatan, lakukan tugas yang disarankan di [Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi](#).
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Pemeriksaan Kondisi.
4. Jika Anda ingin memperbarui pemeriksaan kondisi yang ada, pilih pemeriksaan kondisi, lalu pilih Edit Pemeriksaan kondisi.

Jika Anda ingin membuat pemeriksaan kondisi, pilih Buat Pemeriksaan kondisi. Untuk informasi lebih lanjut tentang setiap pengaturan, pindahkan penunjuk mouse ke atas labelnya untuk melihat kiat alat.

5. Masukkan nilai yang berlaku. Perhatikan bahwa beberapa nilai tidak dapat diubah setelah Anda membuat pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#).
6. Pilih Buat Pemeriksaan Kondisi.

Note

Route 53 menganggap pemeriksaan kondisi baru dalam kondisi sehat hingga ada cukup data untuk menentukan status yang sebenarnya, sehat atau tidak sehat. Jika Anda memilih opsi untuk membalikkan status pemeriksaan kondisi, Route 53 menganggap pemeriksaan kondisi baru tidak sehat hingga ada cukup data.

7. Kaitkan pemeriksaan kondisi dengan satu atau beberapa catatan Route 53. Untuk informasi tentang membuat dan memperbarui catatan, lihat [Bekerja dengan catatan](#).

Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi

Saat membuat atau memperbarui pemeriksaan kondisi, Anda menentukan nilai yang berlaku. Perhatikan bahwa Anda tidak dapat mengubah beberapa nilai setelah Anda pemeriksaan kondisi dibuat.

Topik

- [Memantau titik akhir](#)
- [Memantau pemeriksaan kondisi lainnya \(pemeriksaan kondisi yang dihitung\)](#)
- [Memantau CloudWatch alarm](#)
- [Konfigurasi lanjutan \("Pantau Titik Akhir" saja\)](#)
- [Dapatkan notifikasi ketika pemeriksaan kondisi gagal](#)

Nama

Opsional, namun disarankan: Nama yang ingin Anda tetapkan ke pemeriksaan kondisi. Jika Anda menentukan nilai untuk Nama, Route 53 menambahkan tanda ke pemeriksaan kondisi, memberikan nilai Nama ke kunci tanda, dan menetapkan nilai yang Anda tentukan ke nilai tanda. Nilai tanda Nama muncul dalam daftar pemeriksaan kondisi di konsol Route 53, yang memudahkan Anda membedakan berbagai pemeriksaan kondisi.

Untuk informasi selengkapnya tentang penandaan dan pemeriksaan kondisi, lihat [Penamaan dan penandaan pemeriksaan kondisi](#).

Apa yang harus dipantau

Apakah Anda ingin pemeriksaan kondisi ini memantau titik akhir atau status pemeriksaan kondisi lainnya:

- Titik akhir – Route 53 memantau kondisi titik akhir yang Anda tentukan. Anda dapat menentukan titik akhir dengan memberikan nama domain atau alamat IP dan port.

Note

Jika Anda menentukan AWS non-endpoint, dikenakan biaya tambahan. Untuk informasi selengkapnya, termasuk definisi titik akhir AWS, lihat "Pemeriksaan Kondisi" di halaman [Harga Route 53](#).

- Status pemeriksaan kondisi lainnya (pemeriksaan kondisi yang dihitung) – Route 53 menentukan apakah pemeriksaan kondisi ini sehat berdasarkan status pemeriksaan kondisi lain yang Anda tentukan. Anda juga menentukan berapa banyak pemeriksaan kondisi yang harus sehat agar pemeriksaan kondisi ini dianggap sehat.
- Status aliran data CloudWatch alarm - Route 53 menentukan apakah pemeriksaan kesehatan ini sehat dengan memantau aliran data untuk CloudWatch alarm.

Memantau titik akhir

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Jika Anda ingin pemeriksaan kondisi ini memantau titik akhir, tentukan nilai berikut:

- Tentukan titik akhir dengan
- Alamat IP
- Nama domain

Tentukan titik akhir dengan

Apakah Anda ingin menentukan titik akhir menggunakan alamat IP atau menggunakan nama domain.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Tentukan titik akhir dengan.

Alamat IP (Khusus "Tentukan titik akhir dengan alamat IP")

Pilih protokol di drop-down, masukkan alamat IP, port, dan jalur di kotak teks.

- Protokol dapat berupa salah satu dari yang berikut:

HTTP – Route 53 mencoba membuat koneksi TCP. Jika berhasil, Route 53 mengirimkan permintaan HTTP dan menunggu kode status HTTP 2xx atau 3xx.

- HTTPS – Route 53 mencoba membuat koneksi TCP. Jika berhasil, Route 53 mengirimkan permintaan HTTPS dan menunggu kode status HTTP 2xx atau 3xx.

Important

Jika Anda memilih HTTPS, titik akhir harus mendukung TLS v1.0, v1.1, atau v1.2.

Anda akan dikenakan biaya tambahan jika memilih HTTPS untuk nilai Protokol. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

- TCP – Route 53 mencoba membuat koneksi TCP.

Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Protokol.

Untuk alamat IP Anda dapat memasukkan IPv4 atau IPv6 alamat titik akhir yang Anda inginkan Route 53 untuk melakukan pemeriksaan kesehatan, jika Anda memilih Tentukan titik akhir berdasarkan alamat IP.

Route 53 tidak dapat memeriksa kondisi titik akhir yang memiliki rentang alamat IP lokal, privat, tidak dapat dirutekan, atau multicast. Untuk informasi selengkapnya tentang alamat IP yang tidak dapat dibuat pemeriksaan kondisinya, lihat dokumen berikut:

- [RFC 5735, Alamat Penggunaan Khusus IPv4](#)
- [RFC 6598, IPv4 Awalan yang dicadangkan IANA](#) untuk Ruang Alamat Bersama.
- [RFC 5156, Alamat Penggunaan Khusus IPv6](#)

Jika titik akhir adalah EC2 instans Amazon, sebaiknya Anda membuat alamat IP Elastis, mengaitkannya dengan EC2 instans Anda, dan menentukan alamat IP Elastis. Tindakan ini memastikan bahwa alamat IP instans Anda tidak akan pernah berubah. Untuk informasi selengkapnya, lihat [Alamat IP Elastis \(EIP\)](#) di Panduan EC2 Pengguna Amazon.

Jika Anda menghapus EC2 instans Amazon, pastikan Anda juga menghapus pemeriksaan kesehatan yang terkait dengan EIP. Untuk informasi selengkapnya, lihat [Praktik terbaik untuk pemeriksaan kondisi Amazon Route 53](#).

 Note

Jika Anda menentukan AWS non-endpoint, dikenakan biaya tambahan. Untuk informasi selengkapnya, termasuk definisi titik akhir AWS, lihat "Pemeriksaan Kondisi" di halaman [Harga Route 53](#).

Untuk port Anda memasukkan port pada titik akhir di mana Anda ingin Route 53 melakukan pemeriksaan kesehatan.

Untuk jalur (Hanya Protokol HTTP dan HTTPS) Anda memasukkan jalur yang ingin Anda minta Route 53 saat melakukan pemeriksaan kesehatan. Path dapat berupa nilai apa pun yang titik akhir Anda akan mengembalikan kode status HTTP 2xx atau 3xx ketika titik akhir sehat, seperti `file/.html? docs/route53-health-check.html`. You can also include query string parameters, for example, `/welcome language=jp&login=y`. Jika Anda tidak menyertakan karakter garis miring (/), Route 53 secara otomatis menambahkannya.

Nama domain (Khusus "Tentukan titik akhir dengan nama domain", Semua Protokol)

Nama domain (`example.com`) atau nama subdomain (`backend.example.com`) titik akhir yang akan dilakukan pemeriksaan kondisi oleh Route 53, jika Anda memilih Tentukan titik akhir dengan nama domain.

Jika Anda memilih untuk menentukan titik akhir dengan nama domain, Route 53 mengirimkan kueri DNS untuk menyelesaikan nama domain yang Anda tentukan di Nama domain pada interval yang Anda tentukan di Interval permintaan. Menggunakan alamat IP yang dikembalikan DNS, Route 53 kemudian memeriksa kondisi titik akhir.

 Note

Jika Anda menentukan titik akhir berdasarkan nama domain, Route 53 hanya menggunakan IPv4 untuk mengirim pemeriksaan kesehatan ke titik akhir. Jika tidak ada catatan dengan jenis A untuk nama yang Anda tentukan bagi Nama Domain, pemeriksaan kondisi gagal dengan kesalahan "resolusi DNS gagal".

Jika ingin memeriksa kondisi failover, geolokasi, geoproximity, latensi, multinilai, atau catatan tertimbang, dan Anda memilih untuk menentukan titik akhir dengan nama domain, kami sarankan Anda membuat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk `www.example.com`. Untuk nilai Nama domain, tentukan nama domain server (seperti `us-east-2-www.example.com`), bukan nama catatan (`www.example.com`).

 Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Di samping itu, jika nilai Protokol adalah HTTP atau HTTPS, Route 53 meneruskan nilai Nama domain pada header Host seperti yang telah dijelaskan di Nama Host dalam daftar ini. Jika nilai Protokol adalah TCP, Route 53 tidak meneruskan header Host.

 Note

Jika Anda menentukan AWS non-endpoint, dikenakan biaya tambahan. Untuk informasi selengkapnya, termasuk definisi titik akhir AWS, lihat "Pemeriksaan Kondisi" di halaman [Harga Route 53](#).

Old console

Jika Anda ingin pemeriksaan kondisi ini memantau titik akhir, tentukan nilai berikut:

- Tentukan titik akhir dengan
- Protokol
- Alamat IP
- Nama host
- Port
- Nama domain
- Jalur

Tentukan titik akhir dengan

Apakah Anda ingin menentukan titik akhir menggunakan alamat IP atau menggunakan nama domain.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Tentukan titik akhir dengan.

Protokol

Metode yang digunakan Route 53 untuk memeriksa kondisi titik akhir:

- HTTP – Route 53 mencoba membuat koneksi TCP. Jika berhasil, Route 53 mengirimkan permintaan HTTP dan menunggu kode status HTTP 2xx atau 3xx.
- HTTPS – Route 53 mencoba membuat koneksi TCP. Jika berhasil, Route 53 mengirimkan permintaan HTTPS dan menunggu kode status HTTP 2xx atau 3xx.

Important

Jika Anda memilih HTTPS, titik akhir harus mendukung TLS v1.0, v1.1, atau v1.2.

Anda akan dikenakan biaya tambahan jika memilih HTTPS untuk nilai Protokol. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

- TCP – Route 53 mencoba membuat koneksi TCP.

Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Protokol.

Alamat IP (Khusus "Tentukan titik akhir dengan alamat IP")

IPv6 Alamat IPv4 atau titik akhir yang Anda inginkan Route 53 untuk melakukan pemeriksaan kesehatan, jika Anda memilih Tentukan titik akhir berdasarkan alamat IP.

Route 53 tidak dapat memeriksa kondisi titik akhir yang memiliki rentang alamat IP lokal, privat, tidak dapat dirutekan, atau multicast. Untuk informasi selengkapnya tentang alamat IP yang tidak dapat dibuat pemeriksaan kondisinya, lihat dokumen berikut:

- [RFC 5735, Alamat Penggunaan Khusus IPv4](#)
- [RFC 6598, IPv4 Awalan yang dicadangkan IANA](#) untuk Ruang Alamat Bersama.

- [RFC 5156, Alamat Penggunaan Khusus IPv6](#)

Jika titik akhir adalah EC2 instans Amazon, sebaiknya Anda membuat alamat IP Elastis, mengaitkannya dengan EC2 instans Anda, dan menentukan alamat IP Elastis. Tindakan ini memastikan bahwa alamat IP instans Anda tidak akan pernah berubah. Untuk informasi selengkapnya, lihat [Alamat IP Elastis \(EIP\)](#) di Panduan EC2 Pengguna Amazon.

Jika Anda menghapus EC2 instans Amazon, pastikan Anda juga menghapus pemeriksaan kesehatan yang terkait dengan EIP. Untuk informasi selengkapnya, lihat [Praktik terbaik untuk pemeriksaan kondisi Amazon Route 53](#).

 Note

Jika Anda menentukan AWS non-endpoint, dikenakan biaya tambahan. Untuk informasi selengkapnya, termasuk definisi titik akhir AWS, lihat "Pemeriksaan Kondisi" di halaman [Harga Route 53](#).

Nama host (Khusus "Tentukan titik akhir dengan alamat IP", Khusus Protokol HTTP dan HTTPS)

Nilai yang ingin diteruskan Route 53 pada header Host di pemeriksaan kondisi HTTP dan HTTPS. Biasanya ini adalah nama DNS yang sepenuhnya memenuhi syarat situs web tempat Route 53 melakukan pemeriksaan kondisi. Ketika Route 53 memeriksa kondisi titik akhir, berikut adalah caranya menyusun header Host:

- Jika Anda menentukan nilai **80** untuk Port dan HTTP untuk Protokol, Route 53 meneruskan header Host yang berisi nilai Nama host ke titik akhir.
- Jika Anda menentukan nilai **443** untuk Port dan HTTPS untuk Protokol, Route 53 meneruskan header Host yang berisi nilai Nama host ke titik akhir.
- Jika Anda menentukan nilai lain untuk Port dan HTTP atau HTTPS untuk Protokol, Route 53 meneruskan ke titik akhir Host header yang berisi nilai *Host name:Port*.

Jika Anda memilih untuk menentukan titik akhir dengan alamat IP dan tidak menentukan nilai untuk Nama Host, Route 53 menggantikan nilai Alamat IP pada header Host di setiap kasus sebelumnya.

Port

Port pada titik akhir tempat Route 53 melakukan pemeriksaan kondisi.

Nama domain (Khusus "Tentukan titik akhir dengan nama domain", Semua Protokol)

Nama domain (example.com) atau nama subdomain (backend.example.com) titik akhir yang akan dilakukan pemeriksaan kondisi oleh Route 53, jika Anda memilih Tentukan titik akhir dengan nama domain.

Jika Anda memilih untuk menentukan titik akhir dengan nama domain, Route 53 mengirimkan kueri DNS untuk menyelesaikan nama domain yang Anda tentukan di Nama domain pada interval yang Anda tentukan di Interval permintaan. Menggunakan alamat IP yang dikembalikan DNS, Route 53 kemudian memeriksa kondisi titik akhir.

Note

Jika Anda menentukan titik akhir berdasarkan nama domain, Route 53 hanya menggunakan IPv4 untuk mengirim pemeriksaan kesehatan ke titik akhir. Jika tidak ada catatan dengan jenis A untuk nama yang Anda tentukan bagi Nama Domain, pemeriksaan kondisi gagal dengan kesalahan "resolusi DNS gagal".

Jika ingin memeriksa kondisi failover, geolokasi, geoproximity, latensi, multinilai, atau catatan tertimbang, dan Anda memilih untuk menentukan titik akhir dengan nama domain, kami sarankan Anda membuat pemeriksaan kondisi terpisah untuk setiap titik akhir. Misalnya, buat pemeriksaan kondisi untuk setiap server HTTP yang melayani konten untuk www.example.com. Untuk nilai Nama domain, tentukan nama domain server (seperti us-east-2-www.example.com), bukan nama catatan (www.example.com).

Important

Dalam konfigurasi ini, jika Anda membuat pemeriksaan kondisi dengan nilai Nama Domain yang sesuai dengan nama catatan lalu mengaitkan pemeriksaan kondisi dengan catatan tersebut, hasil pemeriksaan kondisi tidak dapat diprediksi.

Di samping itu, jika nilai Protokol adalah HTTP atau HTTPS, Route 53 meneruskan nilai Nama domain pada header Host seperti yang telah dijelaskan di Nama Host dalam daftar ini. Jika nilai Protokol adalah TCP, Route 53 tidak meneruskan header Host.

 Note

Jika Anda menentukan AWS non-endpoint, dikenakan biaya tambahan. Untuk informasi selengkapnya, termasuk definisi titik akhir AWS, lihat "Pemeriksaan Kondisi" di halaman [Harga Route 53](#).

Jalur (Khusus Protokol HTTP dan HTTPS)

Jalur yang Anda inginkan untuk diminta Route 53 saat melakukan pemeriksaan kondisi. Jalur dapat menjadi nilai apa pun yang akan dikembalikan titik akhir sebagai kode status HTTP 2xx atau 3xx ketika titik akhir sehat, seperti file `/docs/route53-health-check.html`. Anda juga dapat menyertakan parameter string kueri, misalnya, `/welcome.html?language=jp&login=y`. Jika Anda tidak menyertakan karakter garis miring (/), Route 53 akan menambahkannya secara otomatis.

Memantau pemeriksaan kondisi lainnya (pemeriksaan kondisi yang dihitung)

 Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Jika Anda ingin pemeriksaan kondisi ini memantau status pemeriksaan kondisi lainnya, tentukan nilai berikut:

- Pemeriksaan kondisi untuk memantau
- Laporkan sehat ketika

Pemeriksaan kondisi untuk memantau

Pemeriksaan kondisi yang Anda inginkan untuk dipantau Route 53 guna menentukan kondisi pemeriksaan kondisi ini.

Anda dapat menambahkan hingga 256 pemeriksaan kondisi ke Pemeriksaan kondisi yang dipantau. Untuk menghapus pemeriksaan kondisi dari daftar, pilih x di sebelah kanan sorotan pemeriksaan kondisi tersebut.

Note

Anda tidak dapat mengonfigurasi pemeriksaan kondisi yang dihitung untuk memantau kondisi pemeriksaan kondisi lain yang dihitung.

Jika Anda menonaktifkan pemeriksaan kondisi yang dipantau oleh pemeriksaan kondisi yang dihitung, Route 53 menganggap pemeriksaan kondisi yang dinonaktifkan menjadi sehat karena layanan menghitung apakah pemeriksaan kondisi dihitung sehat. Jika Anda ingin pemeriksaan kondisi yang dinonaktifkan dianggap tidak sehat, pilih kotak centang **Balikkan status pemeriksaan kondisi**.

Laporkan sehat ketika

Perhitungan yang Anda inginkan untuk dilakukan Route 53 guna menentukan apakah pemeriksaan kondisi ini sehat:

- Laporkan sehat jika setidaknya x dari y pemeriksaan kondisi yang dipilih sehat – Route 53 menganggap pemeriksaan kondisi ini sehat ketika jumlah pemeriksaan kondisi tertentu yang Anda tambahkan ke Pemeriksaan kondisi yang dipantau sehat. Perhatikan hal berikut:
 - Jika Anda menentukan angka lebih besar dari jumlah pemeriksaan kondisi di Pemeriksaan kondisi yang dipantau, Route 53 selalu menganggap pemeriksaan kondisi ini tidak sehat.
 - Jika Anda menentukan 0, Route 53 selalu menganggap pemeriksaan kondisi ini sehat.
- Laporkan sehat jika setidaknya semua pemeriksaan kondisi sehat (DAN) – Route 53 menganggap pemeriksaan kondisi ini sehat hanya ketika semua pemeriksaan kondisi yang Anda tambahkan ke Pemeriksaan kondisi yang dipantau sehat.
- Laporkan sehat jika satu atau lebih pemeriksaan kondisi sehat (ATAU) – Route 53 menganggap pemeriksaan kondisi ini sehat ketika setidaknya satu pemeriksaan kondisi yang Anda tambahkan ke Pemeriksaan kondisi yang dipantau sehat.

Old console

Jika Anda ingin pemeriksaan kondisi ini memantau status pemeriksaan kondisi lainnya, tentukan nilai berikut:

- Pemeriksaan kondisi untuk memantau
- Laporkan sehat ketika
- Membalikkan status pemeriksaan kondisi
- Nonaktif

Pemeriksaan kondisi untuk memantau

Pemeriksaan kondisi yang Anda inginkan untuk dipantau Route 53 guna menentukan kondisi pemeriksaan kondisi ini.

Anda dapat menambahkan hingga 256 pemeriksaan kondisi ke Pemeriksaan kondisi yang dipantau. Untuk menghapus pemeriksaan kondisi dari daftar, pilih x di sebelah kanan sorotan pemeriksaan kondisi tersebut.

Note

Anda tidak dapat mengonfigurasi pemeriksaan kondisi yang dihitung untuk memantau kondisi pemeriksaan kondisi lain yang dihitung.

Jika Anda menonaktifkan pemeriksaan kondisi yang dipantau oleh pemeriksaan kondisi yang dihitung, Route 53 menganggap pemeriksaan kondisi yang dinonaktifkan menjadi sehat karena layanan menghitung apakah pemeriksaan kondisi dihitung sehat. Jika Anda ingin pemeriksaan kondisi yang dinonaktifkan dianggap tidak sehat, pilih kotak centang Balikkan status pemeriksaan kondisi.

Laporkan sehat ketika

Perhitungan yang Anda inginkan untuk dilakukan Route 53 guna menentukan apakah pemeriksaan kondisi ini sehat:

- Laporkan sehat jika setidaknya x dari y pemeriksaan kondisi yang dipilih sehat – Route 53 menganggap pemeriksaan kondisi ini sehat ketika jumlah pemeriksaan kondisi tertentu yang Anda tambahkan ke Pemeriksaan kondisi yang dipantau sehat. Perhatikan hal berikut:

- Jika Anda menentukan angka lebih besar dari jumlah pemeriksaan kondisi di Pemeriksaan kondisi yang dipantau, Route 53 selalu menganggap pemeriksaan kondisi ini tidak sehat.
- Jika Anda menentukan 0, Route 53 selalu menganggap pemeriksaan kondisi ini sehat.
- Laporkan sehat jika setidaknya semua pemeriksaan kondisi sehat (DAN) – Route 53 menganggap pemeriksaan kondisi ini sehat hanya ketika semua pemeriksaan kondisi yang Anda tambahkan ke Pemeriksaan kondisi yang dipantau sehat.
- Laporkan sehat jika satu atau lebih pemeriksaan kondisi sehat (ATAU) – Route 53 menganggap pemeriksaan kondisi ini sehat ketika setidaknya satu pemeriksaan kondisi yang Anda tambahkan ke Pemeriksaan kondisi yang dipantau sehat.

Balikkan status pemeriksaan kesehatan (hanya konsol lama)

Untuk membalikkan pemeriksaan kesehatan pada konsol baru, lihat [Membalikkan pemeriksaan kesehatan](#).

Pilih apakah Anda ingin Route 53 membalikkan status pemeriksaan kondisi. Jika Anda memilih opsi ini, Route 53 menganggap pemeriksaan kondisi menjadi tidak sehat ketika status sehat dan sebaliknya.

Dinonaktifkan (hanya konsol lama)

Untuk menonaktifkan pemeriksaan kesehatan di konsol baru, lihat [Menonaktifkan atau mengaktifkan pemeriksaan kesehatan](#).

Menghentikan Route 53 melakukan pemeriksaan kondisi. Ketika Anda menonaktifkan pemeriksaan kondisi, Route 53 berhenti mengagregat status pemeriksaan kondisi yang direferensikan.

Setelah Anda menonaktifkan pemeriksaan kondisi, Route 53 menganggap status pemeriksaan kondisi adalah selalu sehat. Jika Anda mengonfigurasi failover DNS, Route 53 terus merutekan lalu lintas ke sumber daya yang sesuai. Jika Anda ingin menghentikan perutean lalu lintas ke sumber daya, balikkan pemeriksaan kesehatan.

 Note

Biaya untuk pemeriksaan kondisi tetap berlaku jika pemeriksaan kondisi dinonaktifkan.

Memantau CloudWatch alarm

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Jika Anda ingin pemeriksaan kesehatan ini memantau status alarm CloudWatch alarm, tentukan nilai berikut:

- CloudWatch alarm
- Status pemeriksaan kondisi

CloudWatch alarm

Pilih CloudWatch alarm yang Anda inginkan untuk digunakan Route 53 untuk menentukan apakah pemeriksaan kesehatan ini sehat. CloudWatch Alarm harus Akun AWS sama dengan pemeriksaan kesehatan.

Note

Route 53 mendukung CloudWatch alarm dengan fitur-fitur berikut:

- Metrik resolusi standar. Metrik resolusi tinggi tidak didukung. Untuk informasi selengkapnya, lihat [Metrik resolusi tinggi](#) di CloudWatch Panduan Pengguna Amazon.
- Statistik: Average, Minimum, Maximum, Sum, dan SampleCount. Perpanjangan statistik tidak didukung.
- Route 53 tidak mendukung alarm “M out of N”. Untuk informasi selengkapnya, lihat [Mengevaluasi alarm](#) di CloudWatch panduan Amazon.

Route 53 tidak mendukung alarm yang menggunakan [matematika metrik](#) untuk menanyakan beberapa CloudWatch metrik.

Jika Anda ingin membuat alarm, lakukan langkah berikut:

1. Pilih Buat. CloudWatch Konsol muncul di tab browser baru.
2. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Membuat atau mengedit CloudWatch alarm](#) di Panduan CloudWatch Pengguna Amazon.
3. Kembali ke tab peramban tempat konsol Route 53 muncul.
4. Pilih tombol refresh di sebelah daftar CloudWatch alarm.
5. Pilih alarm baru dari daftar.

 Important

Jika Anda mengubah pengaturan CloudWatch alarm setelah membuat pemeriksaan kesehatan, Anda harus memperbarui pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat [Memperbarui pemeriksaan kesehatan saat Anda mengubah pengaturan CloudWatch alarm \(pemeriksaan kesehatan yang hanya memantau CloudWatch alarm\)](#).

Status pemeriksaan kondisi

Pilih status pemeriksaan kesehatan (sehat, tidak sehat, atau status terakhir diketahui) ketika CloudWatch memiliki data yang tidak mencukupi untuk menentukan status alarm yang Anda pilih untuk CloudWatch alarm. Jika Anda memilih untuk menggunakan status terakhir yang diketahui, Route 53 menggunakan status pemeriksaan kesehatan dari terakhir kali yang CloudWatch memiliki data yang cukup untuk menentukan status alarm. Untuk pemeriksaan kondisi baru yang tidak memiliki status terakhir, status default untuk pemeriksaan kondisi adalah sehat.

Nilai status pemeriksaan Kesehatan memberikan status sementara ketika aliran data untuk CloudWatch metrik tidak tersedia secara singkat. (Route 53 memantau aliran data untuk CloudWatch metrik, bukan status alarm yang sesuai.) Jika metrik akan sering tidak tersedia atau dalam jangka waktu lama (lebih dari beberapa jam), sebaiknya Anda tidak menggunakan status terakhir.

Old console

Jika Anda ingin pemeriksaan kesehatan ini memantau status alarm CloudWatch alarm, tentukan nilai berikut:

- CloudWatch alarm
- Status pemeriksaan kondisi
- Membalikkan status pemeriksaan kondisi
- Nonaktif

CloudWatch alarm

Pilih CloudWatch alarm yang Anda inginkan untuk digunakan Route 53 untuk menentukan apakah pemeriksaan kesehatan ini sehat. CloudWatch Alarm harus Akun AWS sama dengan pemeriksaan kesehatan.

Note

Route 53 mendukung CloudWatch alarm dengan fitur-fitur berikut:

- Metrik resolusi standar. Metrik resolusi tinggi tidak didukung. Untuk informasi selengkapnya, lihat [Metrik resolusi tinggi](#) di CloudWatch Panduan Pengguna Amazon.
- Statistik: Average, Minimum, Maximum, Sum, dan SampleCount. Perpanjangan statistik tidak didukung.
- Route 53 tidak mendukung alarm “M out of N”. Untuk informasi selengkapnya, lihat [Mengevaluasi alarm](#) di CloudWatch panduan Amazon.

Route 53 tidak mendukung alarm yang menggunakan [matematika metrik](#) untuk menanyakan beberapa CloudWatch metrik.

Jika Anda ingin membuat alarm, lakukan langkah berikut:

1. Pilih Buat. CloudWatch Konsol muncul di tab browser baru.
2. Masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Membuat atau mengedit CloudWatch alarm](#) di Panduan CloudWatch Pengguna Amazon.
3. Kembali ke tab peramban tempat konsol Route 53 muncul.
4. Pilih tombol refresh di sebelah daftar CloudWatch alarm.

5. Pilih alarm baru dari daftar.

Important

Jika Anda mengubah pengaturan CloudWatch alarm setelah membuat pemeriksaan kesehatan, Anda harus memperbarui pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat [Memperbarui pemeriksaan kesehatan saat Anda mengubah pengaturan CloudWatch alarm \(pemeriksaan kesehatan yang hanya memantau CloudWatch alarm\)](#).

Status pemeriksaan kondisi

Pilih status pemeriksaan kesehatan (sehat, tidak sehat, atau status terakhir diketahui) ketika CloudWatch memiliki data yang tidak mencukupi untuk menentukan status alarm yang Anda pilih untuk CloudWatch alarm. Jika Anda memilih untuk menggunakan status terakhir yang diketahui, Route 53 menggunakan status pemeriksaan kesehatan dari terakhir kali yang CloudWatch memiliki data yang cukup untuk menentukan status alarm. Untuk pemeriksaan kondisi baru yang tidak memiliki status terakhir, status default untuk pemeriksaan kondisi adalah sehat.

Nilai status pemeriksaan Kesehatan memberikan status sementara ketika aliran data untuk CloudWatch metrik tidak tersedia secara singkat. (Route 53 memantau aliran data untuk CloudWatch metrik, bukan status alarm yang sesuai.) Jika metrik akan sering tidak tersedia atau dalam jangka waktu lama (lebih dari beberapa jam), sebaiknya Anda tidak menggunakan status terakhir.

Balikkan status pemeriksaan kesehatan (hanya konsol lama)

Untuk membalikkan pemeriksaan kesehatan pada konsol baru, lihat [Membalikkan pemeriksaan kesehatan](#).

Pilih apakah Anda ingin Route 53 membalikkan status pemeriksaan kondisi. Jika Anda memilih opsi ini, Route 53 menganggap pemeriksaan kondisi menjadi tidak sehat ketika status sehat dan sebaliknya.

Dinonaktifkan (hanya konsol lama)

Untuk menonaktifkan pemeriksaan kesehatan di konsol baru, lihat [Menonaktifkan atau mengaktifkan pemeriksaan kesehatan](#).

Menghentikan Route 53 melakukan pemeriksaan kondisi. Saat Anda menonaktifkan pemeriksaan kesehatan, Route 53 berhenti memantau CloudWatch metrik yang sesuai.

Setelah Anda menonaktifkan pemeriksaan kondisi, Route 53 menganggap status pemeriksaan kondisi adalah selalu sehat. Jika Anda mengonfigurasi failover DNS, Route 53 terus merutekan lalu lintas ke sumber daya yang sesuai. Jika Anda ingin menghentikan perutean lalu lintas ke sumber daya, balikkan pemeriksaan kesehatan..

 Note

Biaya untuk pemeriksaan kondisi tetap berlaku jika pemeriksaan kondisi dinonaktifkan.

Konfigurasi lanjutan ("Pantau Titik Akhir" saja)

 Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

- [Konsol baru](#)
- [Konsol lama](#)

New console

- Interval Permintaan
- Ambang batas kegagalan
- Pencocokan string
- Cari string
- Grafik latensi
- Aktifkan SNI
- Nama host

Interval permintaan

Jumlah detik antara waktu ketika setiap pemeriksa kondisi Route 53 mendapat respons dari titik akhir Anda dan waktu ketika mengirimkan permintaan pemeriksaan kondisi berikutnya. Jika Anda memilih interval 30 detik, setiap pemeriksa kondisi Route 53 di pusat data di seluruh dunia akan mengirimkan permintaan pemeriksaan kondisi ke titik akhir Anda setiap 30 detik. Rata-rata, titik akhir Anda akan menerima permintaan pemeriksaan kondisi setiap dua detik. Jika Anda memilih interval 10 detik, titik akhir akan menerima permintaan lebih dari satu kali per detik.

Perhatikan bahwa pemeriksa kondisi Route 53 di pusat data yang berbeda tidak berkoordinasi satu sama lain, sehingga terkadang Anda akan melihat beberapa permintaan per detik terlepas dari interval yang dipilih, diikuti beberapa detik tanpa pemeriksaan kondisi sama sekali.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Interval permintaan.

Note

Anda akan dikenakan biaya tambahan jika memilih Cepat (10 detik) untuk nilai Interval permintaan. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Ambang batas kegagalan

Jumlah pemeriksaan kondisi titik akhir berturut-turut yang harus lolos atau gagal agar Route 53 dapat mengubah status titik akhir saat ini dari tidak sehat menjadi sehat atau sebaliknya. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Pencocokan string (Khusus HTTP dan HTTPS)

Jika Anda ingin Route 53 untuk menentukan kondisi titik akhir dengan mengirimkan permintaan HTTP atau HTTPS ke titik akhir dan mencari string tertentu dalam isi respons. Jika isi respons berisi nilai yang Anda tentukan di Cari string, Route 53 menganggap titik akhir sehat. Jika tidak, atau jika titik akhir tidak merespons, Route 53 menganggap titik akhir tidak sehat. Seluruh pencarian string harus muncul pada 5.120 byte pertama dari isi respons.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Pencocokan string.

 Note

Anda akan dikenakan biaya tambahan jika memilih Ya untuk nilai Pencocokan string. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Bagaimana pemeriksa kesehatan menangani respons terkompresi

Jika titik akhir adalah web server yang mengembalikan respons terkompresi, pemeriksa kondisi Route 53 akan membuka kompresi respons sebelum memeriksa pencarian string yang ditentukan hanya jika server web mengompresi respons menggunakan algoritme kompresi yang didukung pemeriksa kondisi. Pemeriksa kondisi mendukung algoritme kompresi berikut:

- Gzip
- Deflate

Jika respons dikompresi menggunakan algoritme lain, pemeriksa kondisi tidak dapat membuka kompresi respons sebelum mencari string. Dalam kasus ini, pencarian hampir selalu gagal, dan Route 53 akan mempertimbangkan titik akhir tidak sehat

Cari string (Hanya Ketika "Pencocokan string" diaktifkan)

String yang Anda inginkan untuk dicari Route 53 dalam isi respons dari titik akhir Anda. Panjang maksimalnya adalah 255 karakter.

Route 53 peka huruf besar kecil saat mencari Caro string dalam isi respons.

Grafik latensi

Pilih apakah Anda ingin Route 53 mengukur latensi antara pemeriksa kesehatan di beberapa AWS Wilayah dan titik akhir Anda. Jika Anda memilih opsi ini, grafik CloudWatch latensi muncul di tab Latensi pada halaman Pemeriksaan Kesehatan di konsol Route 53. Jika pemeriksa kondisi Route 53 tidak dapat terhubung ke titik akhir, Route 53 tidak dapat menampilkan grafik latensi untuk titik akhir tersebut.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Pengukuran latensi.

 Note

Anda akan dikenakan biaya tambahan jika Route 53 dikonfigurasi untuk mengukur latensi antara pemeriksa kondisi dan titik akhir. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Aktifkan SNI (Khusus HTTPS)

Menentukan apakah Anda ingin Route 53 mengirimkan nama host ke titik akhir dalam pesan `client_hello` selama negosiasi TLS. Hal ini memungkinkan endpoint untuk menanggapi permintaan HTTPS dengan SSL/TLS sertifikat yang berlaku.

Beberapa titik akhir mengharuskan permintaan HTTPS menyertakan nama host dalam pesan `client_hello`. Jika Anda tidak mengaktifkan SNI, status pemeriksaan kesehatan mungkin menunjukkan kegagalan. Pesan kesalahan akan tergantung pada bagaimana server dikonfigurasi untuk menanggapi permintaan yang tidak mengandung informasi SNI. Pemeriksaan kesehatan juga dapat memiliki status kegagalan karena alasan lain. Jika SNI diaktifkan dan Anda masih mendapatkan kesalahan, periksa konfigurasi SSL/TLS di titik akhir Anda dan konfirmasi bahwa sertifikat Anda valid.

Perhatikan persyaratan berikut:

- Titik akhir harus mendukung SNI.
- SSL/TLS Sertifikat pada titik akhir Anda menyertakan nama domain di Common Name lapangan dan mungkin beberapa lagi di Subject Alternative Names lapangan. Salah satu nama domain dalam sertifikat harus sesuai dengan nilai yang Anda tentukan untuk Nama host.

Wilayah pemeriksaan kondisi

Pilih apakah Anda ingin Route 53 memeriksa kondisi titik akhir menggunakan pemeriksa kondisi di wilayah yang direkomendasikan atau menggunakan pemeriksa kondisi di wilayah yang Anda tentukan.

Jika Anda memperbarui pemeriksaan kondisi untuk menghapus wilayah yang telah melakukan pemeriksaan kondisi, Route 53 terus melakukan pemeriksaan dari wilayah tersebut hingga satu jam. Hal ini memastikan bahwa beberapa pemeriksa kondisi selalu memeriksa titik akhir (misalnya, jika Anda mengganti tiga wilayah dengan empat wilayah yang berbeda).

Jika Anda memilih Sesuaikan, pilih x pada wilayah untuk menghapusnya. Klik spasi di bagian bawah daftar untuk menambahkan wilayah kembali ke daftar. Anda harus menentukan setidaknya tiga wilayah.

Nama host (Khusus "Tentukan titik akhir dengan alamat IP", Khusus Protokol HTTP dan HTTPS)

Nilai yang ingin diteruskan Route 53 pada header Host di pemeriksaan kondisi HTTP dan HTTPS. Biasanya ini adalah nama DNS yang sepenuhnya memenuhi syarat situs web tempat Route 53 melakukan pemeriksaan kondisi. Ketika Route 53 memeriksa kondisi titik akhir, berikut adalah caranya menyusun header Host:

- Jika Anda menentukan nilai **80** untuk Port dan HTTP untuk Protokol, Route 53 meneruskan header Host yang berisi nilai Nama host ke titik akhir.
- Jika Anda menentukan nilai **443** untuk Port dan HTTPS untuk Protokol, Route 53 meneruskan ke titik akhir Host header yang berisi nilai nama Host.
- Jika Anda menentukan nilai lain untuk Port dan HTTP atau HTTPS untuk Protokol, Route 53 meneruskan ke titik akhir Host header yang berisi nilai *Host name:Port*.

Jika Anda memilih untuk menentukan titik akhir dengan alamat IP dan tidak menentukan nilai untuk Nama Host, Route 53 menggantikan nilai Alamat IP pada header Host di setiap kasus sebelumnya.

Old console

Jika memilih opsi untuk memantau titik akhir, Anda juga dapat menentukan pengaturan berikut:

- Interval Permintaan
- Ambang batas kegagalan
- Pencocokan string
- String pencarian
- Grafik latensi
- Aktifkan SNI
- Pemeriksa Kesehatan Wilayah
- Membalikkan status pemeriksaan kondisi
- Nonaktif

Interval permintaan

Jumlah detik antara waktu ketika setiap pemeriksa kondisi Route 53 mendapat respons dari titik akhir Anda dan waktu ketika mengirimkan permintaan pemeriksaan kondisi berikutnya. Jika Anda memilih interval 30 detik, setiap pemeriksa kondisi Route 53 di pusat data di seluruh dunia akan mengirimkan permintaan pemeriksaan kondisi ke titik akhir Anda setiap 30 detik. Rata-rata, titik akhir Anda akan menerima permintaan pemeriksaan kondisi setiap dua detik. Jika Anda memilih interval 10 detik, titik akhir akan menerima permintaan lebih dari satu kali per detik.

Perhatikan bahwa pemeriksa kondisi Route 53 di pusat data yang berbeda tidak berkoordinasi satu sama lain, sehingga terkadang Anda akan melihat beberapa permintaan per detik terlepas dari interval yang dipilih, diikuti beberapa detik tanpa pemeriksaan kondisi sama sekali.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Interval permintaan.

Note

Anda akan dikenakan biaya tambahan jika memilih Cepat (10 detik) untuk nilai Interval permintaan. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Ambang batas kegagalan

Jumlah pemeriksaan kondisi titik akhir berturut-turut yang harus lolos atau gagal agar Route 53 dapat mengubah status titik akhir saat ini dari tidak sehat menjadi sehat atau sebaliknya. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Pencocokan string (Khusus HTTP dan HTTPS)

Jika Anda ingin Route 53 untuk menentukan kondisi titik akhir dengan mengirimkan permintaan HTTP atau HTTPS ke titik akhir dan mencari string tertentu dalam isi respons. Jika isi respons berisi nilai yang Anda tentukan di Cari string, Route 53 menganggap titik akhir sehat. Jika tidak, atau jika titik akhir tidak merespons, Route 53 menganggap titik akhir tidak sehat. Seluruh pencarian string harus muncul pada 5.120 byte pertama dari isi respons.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Pencocokan string.

 Note

Anda akan dikenakan biaya tambahan jika memilih Ya untuk nilai Pencocokan string. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Bagaimana pemeriksa kesehatan menangani respons terkompresi

Jika titik akhir adalah web server yang mengembalikan respons terkompresi, pemeriksa kondisi Route 53 akan membuka kompresi respons sebelum memeriksa pencarian string yang ditentukan hanya jika server web mengompresi respons menggunakan algoritme kompresi yang didukung pemeriksa kondisi. Pemeriksa kondisi mendukung algoritme kompresi berikut:

- Gzip
- Deflate

Jika respons dikompresi menggunakan algoritme lain, pemeriksa kondisi tidak dapat membuka kompresi respons sebelum mencari string. Dalam kasus ini, pencarian hampir selalu gagal, dan Route 53 akan mempertimbangkan titik akhir tidak sehat

Cari string (Hanya Ketika "Pencocokan string" diaktifkan)

String yang Anda inginkan untuk dicari Route 53 dalam isi respons dari titik akhir Anda. Panjang maksimalnya adalah 255 karakter.

Route 53 peka huruf besar kecil saat mencari Caro string dalam isi respons.

Grafik latensi

Pilih apakah Anda ingin Route 53 mengukur latensi antara pemeriksa kesehatan di beberapa AWS Wilayah dan titik akhir Anda. Jika Anda memilih opsi ini, grafik CloudWatch latensi muncul di tab Latensi pada halaman Pemeriksaan Kesehatan di konsol Route 53. Jika pemeriksa kondisi Route 53 tidak dapat terhubung ke titik akhir, Route 53 tidak dapat menampilkan grafik latensi untuk titik akhir tersebut.

Setelah membuat pemeriksaan kondisi, Anda tidak dapat mengubah nilai Pengukuran latensi.

 Note

Anda akan dikenakan biaya tambahan jika Route 53 dikonfigurasi untuk mengukur latensi antara pemeriksa kondisi dan titik akhir. Untuk informasi lebih lanjut, lihat [Harga Route 53](#).

Aktifkan SNI (Khusus HTTPS)

Menentukan apakah Anda ingin Route 53 mengirimkan nama host ke titik akhir dalam pesan `client_hello` selama negosiasi TLS. Hal ini memungkinkan endpoint untuk menanggapi permintaan HTTPS dengan SSL/TLS sertifikat yang berlaku.

Beberapa titik akhir mengharuskan permintaan HTTPS menyertakan nama host dalam pesan `client_hello`. Jika Anda tidak mengaktifkan SNI, status pemeriksaan kesehatan mungkin menunjukkan kegagalan. Pesan kesalahan tergantung pada bagaimana server dikonfigurasi untuk menanggapi permintaan yang tidak mengandung informasi SNI. Pemeriksaan kesehatan juga dapat memiliki status kegagalan karena alasan lain. Jika SNI diaktifkan dan Anda masih mendapatkan kesalahan, periksa SSL/TLS konfigurasi pada titik akhir Anda dan konfirmasi bahwa sertifikat Anda valid.

Perhatikan persyaratan berikut:

- Titik akhir harus mendukung SNI.
- SSL/TLS Sertifikat pada titik akhir Anda menyertakan nama domain di Common Name lapangan dan mungkin beberapa lagi di Subject Alternative Names lapangan. Salah satu nama domain dalam sertifikat harus sesuai dengan nilai yang Anda tentukan untuk Nama host.

Wilayah pemeriksaan kondisi

Pilih apakah Anda ingin Route 53 memeriksa kondisi titik akhir menggunakan pemeriksa kondisi di wilayah yang direkomendasikan atau menggunakan pemeriksa kondisi di wilayah yang Anda tentukan.

Jika Anda memperbarui pemeriksaan kondisi untuk menghapus wilayah yang telah melakukan pemeriksaan kondisi, Route 53 terus melakukan pemeriksaan dari wilayah tersebut hingga satu jam. Hal ini memastikan bahwa beberapa pemeriksa kondisi selalu memeriksa titik akhir (misalnya, jika Anda mengganti tiga wilayah dengan empat wilayah yang berbeda).

Jika Anda memilih Sesuaikan, pilih x pada wilayah untuk menghapusnya. Klik spasi di bagian bawah daftar untuk menambahkan wilayah kembali ke daftar. Anda harus menentukan setidaknya tiga wilayah.

Balikkan status pemeriksaan kesehatan (hanya konsol lama)

Untuk membalikkan pemeriksaan kesehatan pada konsol baru, lihat [Membalikkan pemeriksaan kesehatan](#).

Pilih apakah Anda ingin Route 53 membalikkan status pemeriksaan kondisi. Jika Anda memilih opsi ini, Route 53 menganggap pemeriksaan kesehatan tidak sehat ketika statusnya sehat dan sebaliknya. Misalnya, Anda mungkin ingin Route 53 menganggap pemeriksaan kondisi tidak sehat jika Anda mengonfigurasi pencocokan string dan titik akhir mengembalikan nilai tertentu.

Dinonaktifkan (hanya konsol lama)

Untuk menonaktifkan pemeriksaan kesehatan di konsol baru, lihat [Menonaktifkan atau mengaktifkan pemeriksaan kesehatan](#).

Menghentikan Route 53 melakukan pemeriksaan kondisi. Ketika Anda menonaktifkan pemeriksaan kondisi, Route 53 berhenti mencoba membuat koneksi TCP dengan titik akhir.

Setelah Anda menonaktifkan pemeriksaan kondisi, Route 53 menganggap status pemeriksaan kondisi adalah selalu sehat. Jika Anda mengonfigurasi failover DNS, Route 53 terus merutekan lalu lintas ke sumber daya yang sesuai. Jika Anda ingin menghentikan perutean lalu lintas ke sumber daya, balikkan pemeriksaan kesehatan.

 Note

Biaya untuk pemeriksaan kondisi tetap berlaku jika pemeriksaan kondisi dinonaktifkan.

Dapatkan notifikasi ketika pemeriksaan kondisi gagal

Gunakan opsi berikut untuk mengonfigurasi notifikasi email ketika pemeriksaan kondisi gagal:

- [Create alarm](#)
- [Send notification to](#)
- [Topic name](#)
- [Recipient email addresses](#)

Membuat alarm (Hanya Ketika Membuat Pemeriksaan Kondisi)

Tentukan apakah Anda ingin membuat CloudWatch alarm default. Jika Anda memilih Ya, CloudWatch mengirimkan pemberitahuan Amazon SNS ketika status titik akhir ini berubah menjadi tidak sehat dan Route 53 menganggap titik akhir tidak sehat selama satu menit.

Note

Jika Anda CloudWatch ingin mengirim Anda pemberitahuan Amazon SNS lain ketika status berubah kembali menjadi sehat, Anda dapat membuat alarm lain setelah Anda membuat pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat [Membuat CloudWatch alarm Amazon](#) di Panduan CloudWatch Pengguna Amazon.

Jika Anda ingin membuat alarm untuk pemeriksaan kondisi yang ada atau ingin menerima notifikasi ketika Route 53 menganggap titik akhir tidak sehat selama lebih atau kurang dari satu menit (nilai default), pilih Tidak, dan tambahkan alarm setelah Anda membuat pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

Mengirim notifikasi ke (Hanya Ketika Membuat Alarm)

Tentukan apakah Anda CloudWatch ingin mengirim notifikasi ke topik Amazon SNS yang ada atau ke topik baru:

- Topik SNS yang sudah ada – Pilih nama topik dari daftar. Topik harus berada di Wilayah US East (N. Virginia).
- Topik SNS baru – Masukkan nama untuk topik pada Nama topik, lalu masukkan alamat email yang ingin Anda kirimkan notifikasi di Penerima. Pisahkan beberapa alamat dengan koma (,), titik koma (;), atau spasi.

Route 53 akan membuat topik di Wilayah US East (N. Virginia).

Nama topik (Hanya Ketika Membuat Topik SNS Baru)

Jika Anda menentukan Topik SNS Baru, masukkan nama topik baru.

Alamat email penerima (Hanya Ketika Membuat Topik SNS Baru)

Jika Anda menentukan Topik SNS baru, masukkan alamat email yang ingin Anda kirim notifikasi. Pisahkan beberapa nama dengan koma (,), titik koma (;), atau spasi.

Nilai yang ditampilkan Amazon Route 53 ketika Anda membuat pemeriksaan kondisi

Halaman Buat Pemeriksaan Kondisi menampilkan nilai berikut berdasarkan nilai yang Anda ketik:

URL

URL lengkap (untuk pemeriksaan kondisi HTTP atau HTTPS) atau alamat IP dan port (untuk pemeriksaan kondisi TCP) tujuan pengiriman permintaan Route 53 saat melakukan pemeriksaan kondisi.

Jenis Pemeriksaan Kondisi

Dasar atau Dasar + opsi tambahan berdasarkan pengaturan yang Anda tentukan untuk pemeriksaan kondisi ini. Untuk informasi selengkapnya tentang harga opsi tambahan, lihat [Harga Route 53](#).

Memperbarui pemeriksaan kesehatan saat Anda mengubah pengaturan CloudWatch alarm (pemeriksaan kesehatan yang hanya memantau CloudWatch alarm)

Jika Anda membuat pemeriksaan kesehatan Route 53 yang memantau aliran data untuk CloudWatch alarm dan kemudian Anda memperbarui pengaturan di CloudWatch alarm, Route 53 tidak secara otomatis memperbarui pengaturan alarm di pemeriksaan kesehatan. Jika Anda ingin pemeriksaan kondisi mulai menggunakan pengaturan alarm baru, Anda perlu memperbarui pemeriksaan kondisi.

Note

Untuk memperbarui pemeriksaan kondisi secara terprogram, Anda dapat menggunakan API `UpdateHealthCheck`. Cukup tentukan nilai saat ini untuk `AlarmIdentifier` dan `Region`, dan Route 53 akan mendapatkan pengaturan terbaru dari CloudWatch. Untuk informasi selengkapnya, lihat [UpdateHealthCheck](#) di Referensi API Amazon Route 53.

 Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk memperbarui pemeriksaan kesehatan dengan pengaturan CloudWatch alarm baru

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Pilih ID tertaut untuk pemeriksaan kesehatan yang ingin Anda perbarui.
4. Pilih Edit.

Sebuah catatan menjelaskan bahwa CloudWatch alarm untuk pemeriksaan kesehatan telah berubah. Bidang Detail menampilkan pengaturan alarm baru.

5. Pilih Simpan.

Old console

Untuk memperbarui pemeriksaan kesehatan dengan pengaturan CloudWatch alarm baru (konsol)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Pilih kotak centang pada pemeriksaan kondisi yang ingin Anda perbarui.
4. Pilih Edit pemeriksaan kondisi.

Sebuah catatan menjelaskan bahwa CloudWatch alarm untuk pemeriksaan kesehatan telah berubah. Bidang Detail menampilkan pengaturan alarm baru.

5. Pilih Simpan.

Menonaktifkan atau mengaktifkan pemeriksaan kesehatan

Menonaktifkan pemeriksaan kesehatan menghentikan Route 53 dari melakukan pemeriksaan kesehatan. Ketika Anda menonaktifkan pemeriksaan kondisi, Route 53 berhenti mengagregat status pemeriksaan kondisi yang direferensikan. Setelah Anda menonaktifkan pemeriksaan kondisi, Route 53 menganggap status pemeriksaan kondisi adalah selalu sehat. Jika Anda mengonfigurasi failover DNS, Route 53 terus merutekan lalu lintas ke sumber daya yang sesuai. Jika Anda ingin menghentikan perutean lalu lintas ke sumber daya, ubah nilai Inverted.

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Anda dapat menonaktifkan atau mengaktifkan pemeriksaan kesehatan di konsol lama saat Anda membuat atau mengedit pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#).

Untuk menonaktifkan pemeriksaan kesehatan pada konsol baru, lakukan prosedur berikut.

Untuk menonaktifkan atau mengaktifkan pemeriksaan kesehatan (hanya konsol baru)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Di kolom Tindakan pilih tiga titik dan kemudian Nonaktifkan atau Aktifkan.

Atau, pilih ID tertaut dari pemeriksaan kesehatan yang ingin Anda nonaktifkan atau aktifkan.

4. Pada tabel Konfigurasi, bidang Status menentukan apakah pemeriksaan kesehatan diaktifkan, atau dinonaktifkan.
5. Pilih Nonaktifkan atau Aktifkan untuk menonaktifkan atau mengaktifkan pemeriksaan kesehatan.

Membalikkan pemeriksaan kesehatan

Jika Anda membalikkan pemeriksaan kesehatan, Route 53 menganggap pemeriksaan kesehatan tidak sehat ketika statusnya sehat dan sebaliknya.

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Anda dapat membalikkan pemeriksaan kesehatan di konsol lama saat Anda membuat atau mengedit pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#).

Untuk membalikkan pemeriksaan kesehatan pada konsol baru, lakukan prosedur berikut.

Untuk membalikkan pemeriksaan kesehatan (hanya konsol baru)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Di kolom Actions pilih tiga titik dan kemudian Balikkan.

Atau- pilih ID yang ditautkan dari pemeriksaan kesehatan yang ingin Anda balikkan.

4. Pada tabel Konfigurasi, file Terbalik menentukan apakah pemeriksaan kesehatan terbalik (Ya) atau tidak (Tidak).
5. Pilih Invert untuk membalikkan pemeriksaan kesehatan.

Jika Anda ingin membatalkan status terbalik, dan bidang Terbalik adalah Ya, pilih Balikkan lagi.

Menghapus pemeriksaan kondisi

Untuk menonaktifkan pemeriksaan kesehatan, lakukan prosedur berikut.

Note

Jika Anda menggunakan AWS Cloud Map dan mengonfigurasi AWS Cloud Map untuk membuat pemeriksaan kesehatan Route 53 saat mendaftarkan instance, Anda tidak dapat

menggunakan konsol Route 53 untuk menghapus pemeriksaan kesehatan. Pemeriksaan kondisi dihapus secara otomatis ketika Anda membatalkan pendaftaran instans. Ada penundaan beberapa jam sebelum pemeriksaan kondisi menghilang dari konsol Route 53.

 Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk menghapus pemeriksaan kesehatan

1. Jika Anda menghapus pemeriksaan kondisi yang dikaitkan dengan catatan, lakukan tugas yang disarankan di [Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi](#).
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Pemeriksaan Kesehatan.
4. Pilih ID tertaut dari pemeriksaan kesehatan yang ingin Anda hapus.
5. Pilih Hapus.
6. Masukkan **confirm** di kotak teks dan kemudian pilih Hapus.

Old console

Cara menghapus pemeriksaan kondisi (konsol)

1. Jika Anda menghapus pemeriksaan kondisi yang dikaitkan dengan catatan, lakukan tugas yang disarankan di [Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi](#).
2. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
3. Di panel navigasi, pilih Pemeriksaan Kondisi.
4. Di panel kanan, pilih pemeriksaan kondisi yang ingin Anda hapus.
5. Pilih Hapus Pemeriksaan Kondisi.
6. Pilih Ya, Hapus untuk mengonfirmasi.

Memperbarui atau menghapus pemeriksaan kondisi jika failover DNS dikonfigurasi

Jika ingin memperbarui atau menghapus pemeriksaan kondisi yang dikaitkan dengan catatan, atau ingin mengubah catatan yang dikaitkan dengan pemeriksaan kondisi, Anda harus mempertimbangkan bagaimana perubahan memengaruhi perutean kueri DNS dan konfigurasi failover DNS.

Important

Route 53 tidak mencegah Anda menghapus pemeriksaan kondisi meski pemeriksaan kondisi dikaitkan dengan satu atau lebih catatan. Jika Anda menghapus pemeriksaan kondisi dan tidak memperbarui catatan yang dikaitkan, status pemeriksaan kondisi berikutnya tidak dapat diprediksi dan dapat berubah. Tindakan ini akan memengaruhi perutean kueri DNS untuk konfigurasi failover DNS Anda.

Untuk memperbarui atau menghapus pemeriksaan kondisi yang telah dikaitkan dengan catatan, sebaiknya Anda lakukan tugas berikut:

1. Mengidentifikasi catatan yang terkait dengan pemeriksaan kondisi. Untuk mengidentifikasi catatan yang terkait dengan pemeriksaan kondisi, Anda harus melakukan salah satu hal berikut:

- Meninjau catatan di setiap zona yang di-hosting menggunakan konsol Route 53. Untuk informasi selengkapnya, lihat [Mencantumkan catatan](#).
 - Menjalankan tindakan API `ListResourceRecordSets` di setiap zona yang di-hosting dan meninjau responsnya. Untuk informasi selengkapnya, lihat [ListResourceRecordSets](#) di Referensi API Amazon Route 53.
2. Menilai perubahan perilaku yang akan dihasilkan dari memperbarui atau menghapus pemeriksaan kondisi, atau memperbarui catatan. Berdasarkan penilaian tersebut, tentukan perubahan yang harus dibuat.

Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#)

3. Mengubah pemeriksaan kondisi dan catatan sebagaimana berlaku. Untuk informasi selengkapnya, lihat topik berikut:
- [Membuat dan memperbarui pemeriksaan kondisi](#)
 - [Mengedit catatan](#)
4. Menghapus pemeriksaan kondisi yang tidak lagi digunakan, jika ada. Untuk informasi selengkapnya, lihat [Menghapus pemeriksaan kondisi](#).

Mengonfigurasi aturan router dan firewall untuk pemeriksaan kondisi Amazon Route 53

Ketika memeriksa kondisi titik akhir, Route 53 mengirimkan permintaan HTTP, HTTPS, atau TCP ke alamat IP dan port yang Anda tentukan ketika membuat pemeriksaan kondisi. Agar pemeriksaan kondisi berhasil, aturan router dan firewall harus mengizinkan lalu lintas masuk dari alamat IP yang digunakan pemeriksa kondisi Route 53.

Untuk daftar alamat IP saat ini untuk pemeriksa kesehatan Route 53, untuk server nama Route 53, dan untuk AWS layanan lainnya, lihat [Rentang alamat IP server Amazon Route 53](#).

Di Amazon EC2, kelompok keamanan bertindak sebagai firewall. Untuk informasi selengkapnya, lihat [Grup EC2 keamanan Amazon](#) di Panduan EC2 Pengguna Amazon. Untuk mengonfigurasi grup keamanan Anda agar mengizinkan pemeriksaan kesehatan Route 53, Anda dapat mengizinkan lalu lintas masuk dari setiap rentang alamat IP, atau Anda dapat menggunakan daftar awalan AWS-terkelola.

Untuk menggunakan daftar awalan AWS-managed, ubah grup keamanan Anda untuk mengizinkan lalu lintas masuk `com.amazonaws.<region>.route53-healthchecks`, yang `<region>` merupakan EC2 instans atau sumber Wilayah AWS daya Amazon Anda. Jika Anda menggunakan pemeriksaan kesehatan Route 53 untuk memeriksa IPv6 titik akhir, Anda juga harus mengizinkan lalu lintas masuk dari `com.amazonaws.<region>.ipv6.route53-healthchecks`

Untuk informasi selengkapnya tentang daftar awalan AWS-terkelola, lihat [Bekerja dengan daftar awalan AWS-terkelola di Panduan Pengguna](#) Amazon VPC.

Important

Saat Anda menambahkan alamat IP ke daftar alamat IP yang diizinkan, tambahkan semua alamat IP dalam rentang CIDR untuk setiap AWS Wilayah yang Anda tentukan saat Anda membuat pemeriksaan kesehatan, serta rentang CIDR Global. Anda mungkin melihat bahwa permintaan pemeriksaan kondisi hanya berasal dari satu alamat IP dalam Wilayah. Namun, alamat IP tersebut dapat berubah sewaktu-waktu menjadi alamat IP lain untuk Wilayah tersebut.

Jika Anda ingin memastikan bahwa Anda menyertakan alamat IP pemeriksa kondisi saat ini dan sebelumnya, tambahkan SEMUA rentang alamat IP /26 dan /18 ke daftar alamat IP yang diizinkan. Untuk daftar lengkap, lihat [rentang alamat AWS IP](#) di Referensi Umum AWS. Saat Anda menambahkan daftar awalan AWS-managed ke grup keamanan masuk Anda, secara otomatis menambahkan semua rentang yang diperlukan.

Mengonfigurasi failover DNS

Bila Anda memiliki lebih dari satu sumber daya yang menjalankan fungsi yang sama—misalnya, lebih dari satu server HTTP atau server email—Anda dapat mengonfigurasi Amazon Route 53 untuk memeriksa kondisi sumber daya dan merespons kueri DNS hanya menggunakan sumber daya yang sehat. Misalnya, situs web Anda, `example.com`, di-host di enam server, masing-masing dua dalam tiga pusat data di seluruh dunia. Anda dapat mengonfigurasi Route 53 untuk memeriksa kondisi server tersebut dan untuk menanggapi kueri DNS untuk `example.com` menggunakan hanya server yang saat ini sehat.

Route 53 dapat memeriksa kondisi sumber daya Anda dalam konfigurasi sederhana dan kompleks:

- Dalam konfigurasi sederhana, Anda membuat grup catatan yang semuanya memiliki nama dan jenis yang sama, seperti grup catatan tertimbang dengan jenis A untuk `example.com`. Anda

kemudian mengonfigurasi Route 53 untuk memeriksa kondisi sumber daya yang sesuai. Route 53 merespons kueri DNS berdasarkan kondisi sumber daya Anda. Untuk informasi selengkapnya, lihat [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang sederhana](#).

- Dalam konfigurasi yang lebih kompleks, Anda membuat pohon catatan yang merutekan lalu lintas berdasarkan beberapa kriteria. Misalnya, jika latensi untuk pengguna adalah kriteria yang paling penting, Anda dapat menggunakan catatan alias latensi untuk merutekan lalu lintas ke wilayah yang memberikan latensi terbaik. Catatan alias latensi mungkin memiliki catatan tertimbang di setiap wilayah sebagai target alias. Catatan tertimbang mungkin merutekan lalu lintas ke EC2 instance berdasarkan jenis instance. Seperti konfigurasi sederhana, Anda dapat mengonfigurasi Route 53 untuk merutekan lalu lintas berdasarkan kesehatan sumber daya Anda. Untuk informasi selengkapnya, lihat [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang kompleks](#).

Topik

- [Daftar tugas untuk mengonfigurasi failover DNS](#)
- [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang sederhana](#)
- [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang kompleks](#)
- [Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi](#)
- [Failover active-active dan active-passive](#)
- [Mengonfigurasi failover di zona yang di-hosting secara privat](#)
- [Cara Amazon Route 53 mencegah masalah failover](#)

Daftar tugas untuk mengonfigurasi failover DNS

Untuk menggunakan Route 53 guna mengonfigurasi failover DNS, lakukan tugas berikut:

1. Gambar diagram pohon lengkap dari konfigurasi Anda, dan tunjukkan jenis catatan yang Anda buat (alias tertimbang, failover, latensi, dan sebagainya) untuk setiap simpul. Di bagian atas pohon, tempatkan catatan untuk nama domain, seperti example.com, yang akan digunakan pengguna untuk mengakses situs web atau aplikasi web Anda.

Jenis catatan yang muncul dalam diagram pohon Anda tergantung pada kompleksitas konfigurasi:

- Dalam konfigurasi sederhana, diagram Anda tidak akan menyertakan catatan alias apa pun, atau catatan alias akan merutekan lalu lintas secara langsung ke sumber daya, seperti penyeimbang beban ELB, bukan ke catatan Route 53 lainnya. Untuk informasi selengkapnya, lihat [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang sederhana](#).
- Dalam konfigurasi yang kompleks, diagram Anda akan menyertakan kombinasi catatan alias (seperti alias tertimbang dan alias failover) serta catatan non-alias di pohon multilevel seperti contoh dalam topik [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang kompleks](#).

 Note

Untuk mempercepat dan memudahkan pembuatan catatan bagi konfigurasi perutean yang rumit serta mengaitkan catatan dengan pemeriksaan kondisi, Anda dapat menggunakan editor visual aliran lalu lintas dan menyimpan konfigurasi sebagai kebijakan lalu lintas. Anda kemudian dapat mengaitkan kebijakan lalu lintas dengan satu atau lebih nama domain (seperti example.com) atau nama subdomain (seperti www.example.com), di zona yang di-hosting yang sama atau di beberapa zona yang di-hosting. Selain itu, Anda dapat memulihkan pembaruan jika konfigurasi baru tidak memiliki performa seperti yang Anda harapkan. Untuk informasi selengkapnya, lihat [Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS](#).

Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- [Memilih kebijakan perutean](#)
 - [Memilih antara catatan alias dan nonalias](#)
2. Buat pemeriksaan kesehatan untuk sumber daya yang tidak dapat Anda buat catatan alias, seperti EC2 server Amazon dan server email yang berjalan di pusat data Anda. Anda akan mengaitkan pemeriksaan kondisi ini dengan catatan non-alias.

Untuk informasi selengkapnya, lihat [Membuat, memperbarui, dan menghapus pemeriksaan kondisi](#).

3. Jika perlu, konfigurasi router dan aturan firewall sehingga Route 53 dapat mengirim permintaan reguler ke titik akhir yang Anda tentukan dalam pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Mengonfigurasi aturan router dan firewall untuk pemeriksaan kondisi Amazon Route 53](#).

4. Membuat semua catatan non-alias dalam diagram Anda, dan mengaitkan pemeriksaan kondisi yang Anda buat di langkah 2 dengan catatan yang ada.

Jika Anda mengonfigurasi failover DNS dalam konfigurasi yang tidak menyertakan catatan alias, lewati tugas yang tersisa.

5. Buat catatan alias yang mengarahkan lalu lintas ke AWS sumber daya, seperti penyeimbang beban dan distribusi ELB. CloudFront Jika Anda ingin Route 53 mencoba cabang pohon lain ketika sumber daya tidak sehat, atur nilai Evaluasi Kondisi Target ke Ya untuk setiap catatan alias Anda. (Evaluasi Kesehatan Target tidak didukung untuk beberapa AWS sumber daya.)
6. Mulai dari bagian bawah diagram pohon yang Anda buat di langkah 1, buat catatan alias yang merutekan lalu lintas ke catatan yang Anda buat di langkah 4 dan 5. Jika Anda ingin Route 53 mencoba cabang pohon lain ketika semua catatan non-alias pada cabang pohon Anda tidak sehat, atur nilai Evaluasi Kondisi Target ke Ya untuk setiap catatan alias Anda.

Ingatlah bahwa Anda tidak dapat membuat catatan alias yang merutekan lalu lintas ke catatan lain hingga Anda membuat catatan lainnya.

Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang sederhana

Jika Anda memiliki dua atau lebih sumber daya yang melakukan fungsi yang sama, seperti dua atau lebih server web untuk example.com, Anda dapat menggunakan fitur pemeriksaan kondisi berikut untuk merutekan lalu lintas hanya ke sumber daya yang sehat:

Periksa kesehatan EC2 instans dan sumber daya lainnya (catatan non-alias)

Jika Anda merutekan lalu lintas ke sumber daya yang tidak dapat Anda buat catatan alias, seperti EC2 instance, Anda membuat catatan dan pemeriksaan kesehatan untuk setiap sumber daya. Kemudian kaitkan setiap pemeriksaan kondisi dengan catatan yang ada. Pemeriksaan kondisi secara teratur memeriksa kondisi sumber daya yang sesuai, dan Route 53 merutekan lalu lintas hanya ke sumber daya yang dilaporkan sebagai sehat oleh pemeriksaan kondisi.

Mengevaluasi kesehatan sumber AWS daya (alias catatan)

Jika Anda menggunakan [catatan alias](#) untuk merutekan lalu lintas ke AWS sumber daya yang dipilih, seperti penyeimbang beban ELB, Anda dapat mengonfigurasi Route 53 untuk mengevaluasi kesehatan sumber daya dan merutekan lalu lintas hanya ke sumber daya yang

sehat. Jika Anda mengonfigurasi catatan alias untuk mengevaluasi kondisi sumber daya, Anda tidak perlu membuat pemeriksaan kondisi untuk sumber daya.

Berikut adalah gambaran umum tentang cara mengonfigurasi Route 53 untuk memeriksa kondisi sumber daya Anda dalam konfigurasi yang sederhana:

1. Anda mengidentifikasi sumber daya yang ingin dipantau oleh Route 53. Misalnya, Anda mungkin ingin memantau semua server HTTP yang merespons permintaan `example.com`.
2. Anda membuat pemeriksaan kesehatan untuk sumber daya yang tidak dapat Anda buat catatan alias, seperti EC2 instance atau server di pusat data Anda sendiri. Anda menentukan cara mengirim permintaan pemeriksaan kondisi ke sumber daya: protokol yang digunakan (HTTP, HTTPS, atau TCP), alamat IP dan port yang digunakan, dan, untuk pemeriksaan kondisi HTTP/HTTPS, nama domain serta jalur.

 Note

Jika Anda menggunakan sumber daya yang catatan aliasnya dapat Anda buat, seperti penyeimbang beban ELB, jangan buat pemeriksaan kondisi untuk sumber daya tersebut.

Konfigurasi yang umum adalah membuat satu pemeriksaan kondisi untuk setiap sumber daya dan menggunakan alamat IP yang sama untuk titik akhir pemeriksaan kondisi serta sumber daya. Pemeriksaan kondisi mengirimkan permintaan ke alamat IP yang ditentukan.

 Note

Route 53 tidak dapat memeriksa kondisi sumber daya yang memiliki rentang alamat IP lokal, privat, tidak dapat dirutekan, atau multicast. Untuk informasi selengkapnya tentang alamat IP yang tidak dapat Anda buat pemeriksaan kesehatan, lihat [RFC 5735, IPv4 Alamat Penggunaan Khusus dan RFC 6598](#), [Awalan yang dicadangkan IANA IPv4](#) untuk Ruang Alamat Bersama.

Untuk informasi selengkapnya tentang membuat pemeriksaan kondisi, lihat [Membuat, memperbarui, dan menghapus pemeriksaan kondisi](#).

3. Anda mungkin perlu mengonfigurasi router dan aturan firewall sehingga Route 53 dapat mengirim permintaan reguler ke titik akhir yang Anda tentukan dalam pemeriksaan kondisi.

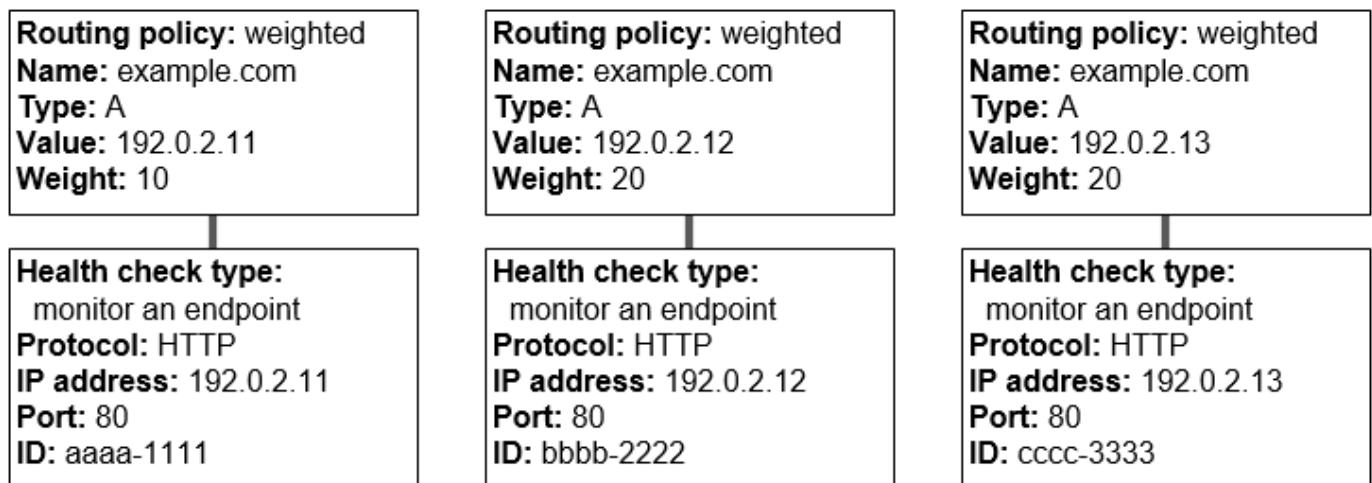
Untuk informasi selengkapnya, lihat [Mengonfigurasi aturan router dan firewall untuk pemeriksaan kondisi Amazon Route 53](#).

4. Anda membuat grup catatan untuk sumber daya, misalnya, grup catatan tertimbang. Anda dapat mencampur catatan alias dan non-alias, tetapi semuanya harus memiliki nilai yang sama untuk Nama, Jenis, dan Kebijakan Perutean.

Cara mengonfigurasi Route 53 untuk memeriksa kondisi sumber daya tergantung pada apakah Anda membuat catatan alias atau catatan non-alias:

- Catatan alias – Menentukan Ya untuk Evaluasi Kondisi Target.
- Catatan non-alias – Mengaitkan pemeriksaan kondisi yang Anda buat di langkah 2 dengan catatan yang sesuai.

Setelah selesai, konfigurasi Anda terlihat mirip dengan diagram berikut, yang hanya mencakup catatan non-alias.



Untuk informasi lebih lanjut tentang membuat catatan menggunakan konsol Route 53, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#).

5. Jika Anda membuat pemeriksaan kondisi, Route 53 secara berkala mengirimkan permintaan ke titik akhir untuk setiap pemeriksaan kondisi; layanan ini tidak melakukan pemeriksaan kondisi saat menerima kueri DNS. Berdasarkan respons, Route 53 memutuskan apakah titik akhir sehat dan menggunakan informasi tersebut untuk menentukan bagaimana merespons kueri. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Route 53 tidak memeriksa kondisi sumber daya yang ditentukan dalam catatan, seperti alamat IP di yang ditentukan dalam catatan A untuk example.com. Ketika Anda mengaitkan pemeriksaan kondisi dengan catatan, Route 53 mulai memeriksa kondisi titik akhir yang Anda tentukan dalam pemeriksaan kondisi. Anda juga dapat mengonfigurasi Route 53 untuk memantau kesehatan pemeriksaan kesehatan lainnya atau memantau aliran data untuk CloudWatch alarm. Untuk informasi selengkapnya, lihat [Jenis pemeriksaan kondisi Amazon Route 53](#).

Inilah yang terjadi saat Route 53 menerima kueri untuk example.com:

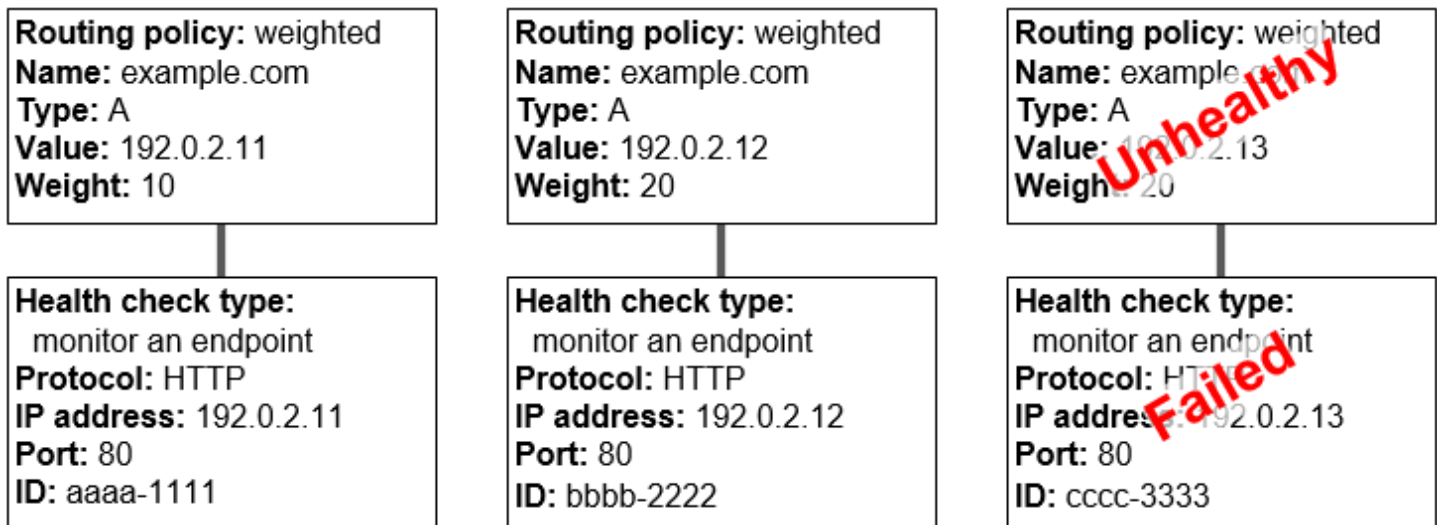
1. Route 53 memilih catatan berdasarkan kebijakan perutean. Dalam hal ini, layanan memilih catatan berdasarkan bobot.
2. Layanan menentukan kondisi saat ini dari catatan yang dipilih dengan memeriksa status pemeriksaan kondisi untuk catatan tersebut.
3. Jika catatan yang dipilih tidak sehat, Route 53 memilih catatan yang berbeda. Kali ini, catatan tidak sehat tidak dipertimbangkan.

Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi](#).

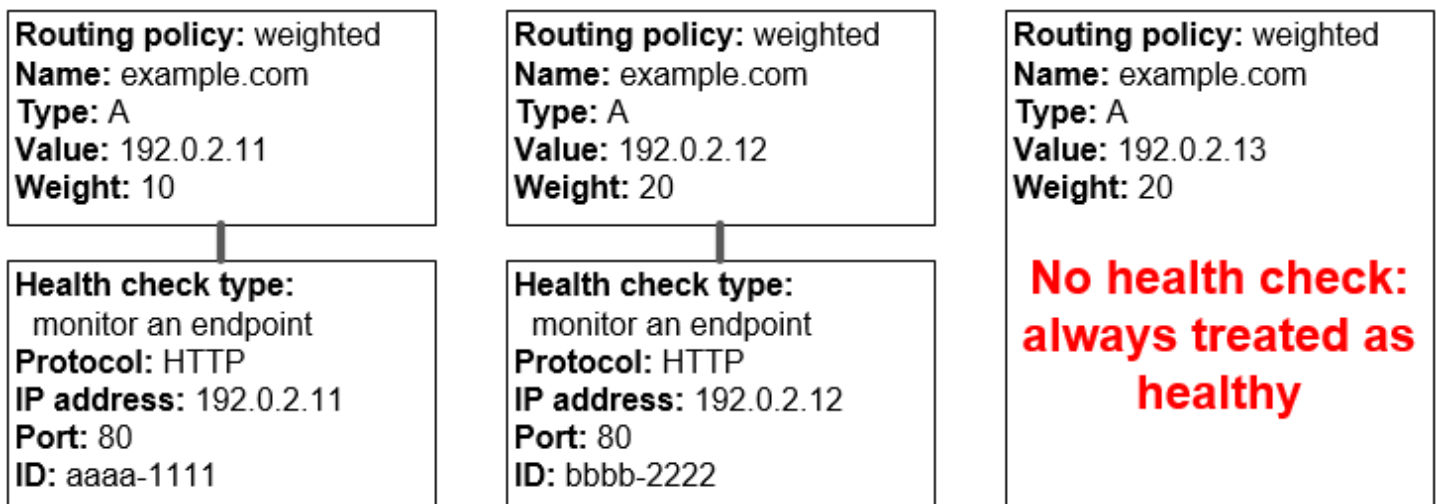
4. Ketika menemukan catatan yang sehat, Route 53 merespons kueri dengan nilai yang ada, seperti alamat IP dalam catatan A.

Contoh berikut menunjukkan grup catatan tertimbang di mana catatan ketiga tidak sehat. Awalnya, Route 53 memilih catatan berdasarkan bobot ketiga catatan. Jika catatan tidak sehat dipilih untuk pertama kalinya, Route 53 memilih catatan lain, namun kali ini menghilangkan bobot catatan ketiga dari kalkulasi:

- Ketika di awal Route 53 memilih di antara ketiga catatan, layanan merespons permintaan menggunakan catatan pertama sekitar 20%, $10/(10 + 20 + 20)$.
- Ketika catatan ketiga dianggap tidak sehat, Route 53 merespons permintaan menggunakan catatan pertama sekitar 33%, $10/(10 + 20)$.



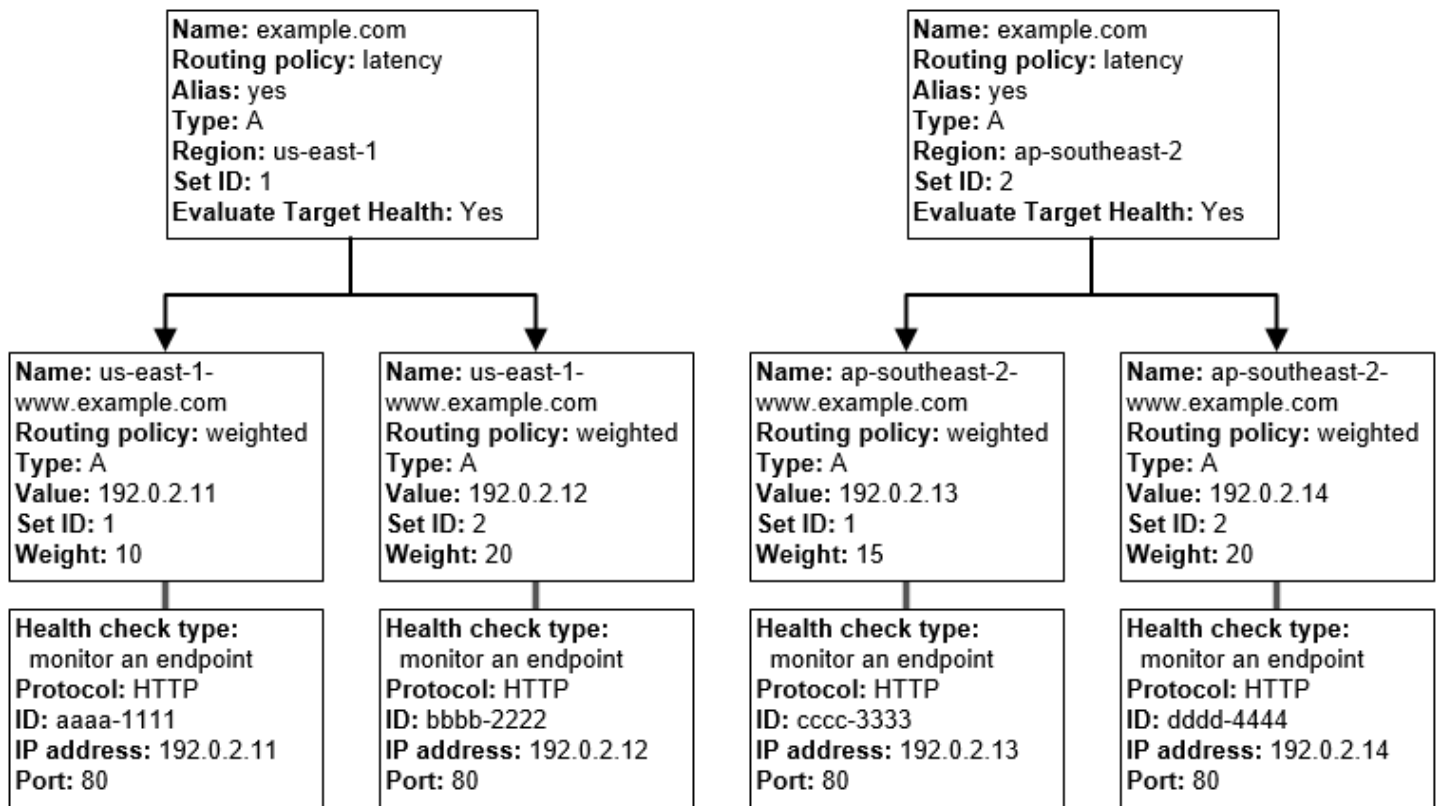
Jika Anda menghilangkan pemeriksaan kondisi dari satu atau lebih catatan dalam grup catatan, Route 53 tidak memiliki cara untuk menentukan kondisi sumber daya yang sesuai. Route 53 menganggap bahwa catatan dalam kondisi sehat.



Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang kompleks

Memeriksa kondisi sumber daya dalam konfigurasi yang kompleks hampir sama seperti dalam konfigurasi yang sederhana. Namun, dalam konfigurasi yang kompleks, Anda menggunakan kombinasi catatan alias (seperti alias tertimbang dan alias failover) serta catatan non-alias untuk membangun pohon keputusan yang memberikan Anda kontrol yang lebih besar atas cara Route 53 merespons permintaan.

Misalnya, Anda mungkin menggunakan data alias latensi untuk memilih wilayah yang dekat dengan pengguna dan menggunakan catatan tertimbang untuk dua atau lebih sumber daya dalam setiap wilayah untuk agar terlindung dari kegagalan titik akhir tunggal atau Availability Zone. Diagram berikut menunjukkan konfigurasi ini.



Begini cara Amazon EC2 dan Route 53 dikonfigurasi. Mari kita mulai dari bagian bawah pohon karena Anda akan membuat catatan dalam urutan tersebut:

- Anda memiliki dua EC2 contoh di masing-masing dari dua wilayah, us-east-1 dan ap-southeast-2. Anda ingin Route 53 untuk mengarahkan lalu lintas ke EC2 instans Anda berdasarkan apakah mereka sehat, sehingga Anda membuat pemeriksaan kesehatan untuk setiap instance. Anda mengonfigurasi setiap pemeriksaan kondisi untuk mengirim permintaan pemeriksaan kondisi ke instans yang sesuai di alamat IP elastis untuk instans tersebut.

Route 53 adalah layanan global, sehingga Anda tidak perlu menentukan wilayah tempat pemeriksaan kondisi dibuat.

- Anda ingin merutekan lalu lintas ke dua instans di setiap wilayah berdasarkan tipe instans, sehingga Anda membuat catatan tertimbang untuk setiap instans dan memberikan bobot ke setiap catatan. (Anda dapat mengubah bobot nanti untuk merutekan lebih banyak atau lebih sedikit lalu lintas ke instans.) Anda juga mengaitkan pemeriksaan kondisi yang ada dengan setiap instans.

Saat membuat catatan, Anda menggunakan nama seperti `us-east-1-www.example.com`. dan `ap-southeast-2-www.example.com`. Anda harus menunggu hingga tiba di puncak pohon untuk dapat memberikan nama ke catatan yang akan digunakan pelanggan guna mengakses situs web atau aplikasi web Anda, seperti `example.com`.

- Anda ingin merutekan lalu lintas ke wilayah yang menyediakan latensi terendah bagi pengguna, jadi Anda memilih [kebijakan perutean](#) latensi untuk catatan di puncak pohon.

Anda ingin merutekan lalu lintas ke catatan di setiap wilayah, tidak langsung ke sumber daya di setiap wilayah (catatan tertimbang sudah melakukannya). Akibatnya, Anda membuat [catatan alias](#) latensi.

Saat membuat catatan alias, Anda memberinya nama yang akan digunakan pengguna untuk mengakses situs web atau aplikasi web Anda, misalnya `example.com`. Catatan alias merutekan lalu lintas untuk `example.com` ke catatan `us-east-1-www.example.com` dan `ap-southeast-2-www.example.com`.

Untuk kedua catatan alias latensi, Anda mengatur nilai Evaluasi Kondisi Target ke Ya. Hal ini menyebabkan Route 53 menentukan apakah ada sumber daya yang sehat di suatu wilayah sebelum mencoba merutekan lalu lintas di sana. Jika tidak ada, Route 53 memilih sumber daya yang sehat di wilayah lain.

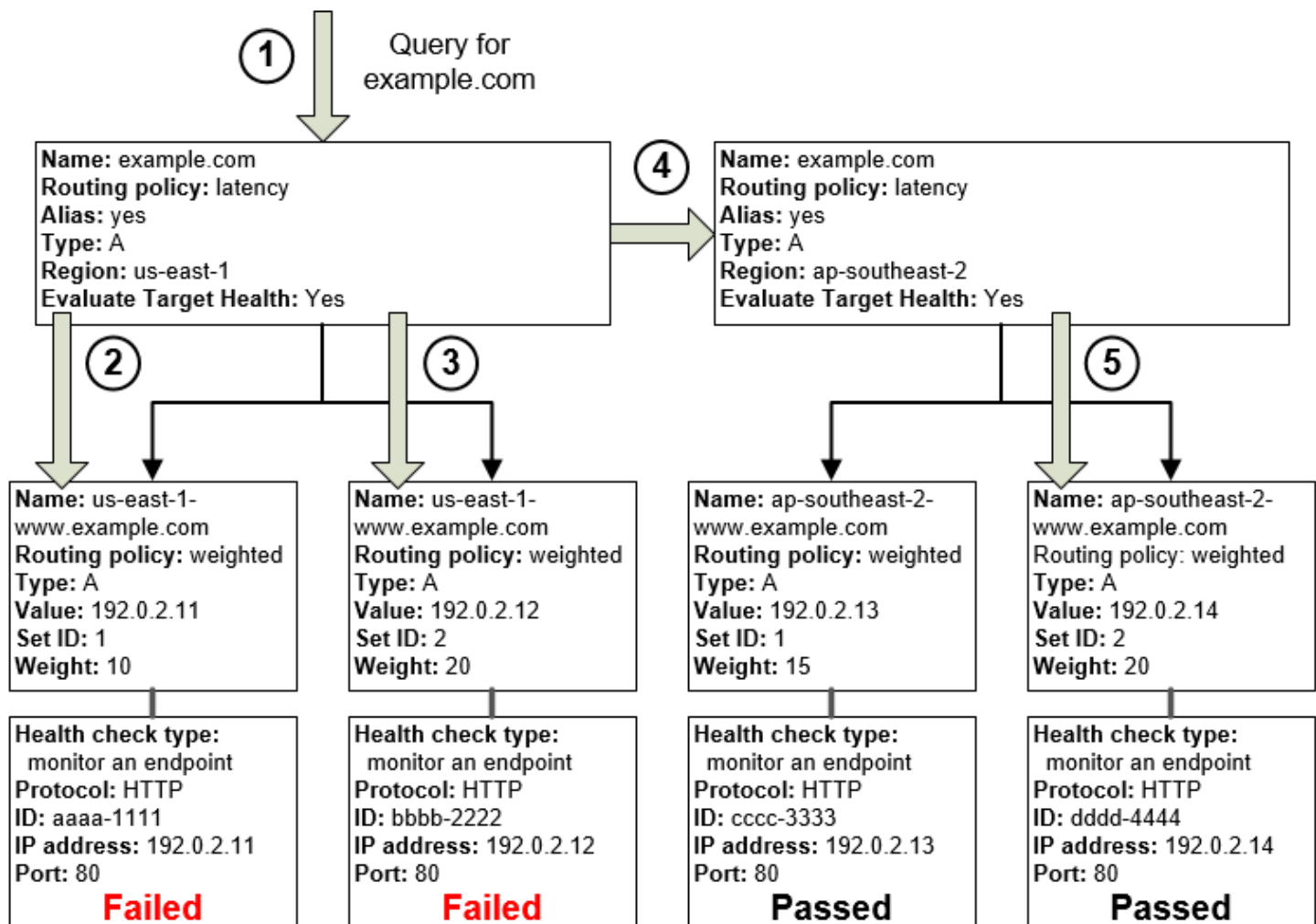


Diagram sebelumnya menggambarkan urutan peristiwa berikut:

1. Route 53 menerima kueri untuk example.com. Berdasarkan latensi untuk pengguna yang membuat permintaan, Route 53 memilih catatan alias latensi untuk wilayah us-east-1.
2. Route 53 memilih catatan tertimbang berdasarkan bobot. Evaluasi Kondisi Target adalah Ya untuk catatan alias latensi, jadi Route 53 memeriksa kondisi catatan tertimbang yang dipilih.
3. Pemeriksaan kondisi gagal, jadi Route 53 memilih catatan tertimbang lain berdasarkan bobotnya dan memeriksa kondisinya. Catatan itu juga tidak sehat.
4. Route 53 keluar dari cabang pohon tersebut, mencari catatan alias latensi dengan latensi terbaik berikutnya, dan memilih catatan untuk ap-southeast-2.
5. Sekali lagi Route 53 memilih catatan berdasarkan bobot, lalu memeriksa kondisi sumber daya yang dipilih. Sumber daya ini sehat, sehingga Route 53 mengembalikan nilai yang ada untuk merespons kueri.

Topik

- [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#)
- [Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?](#)
- [Apa yang terjadi ketika Anda mengatur evaluasi target kondisi ke Tidak?](#)

Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?

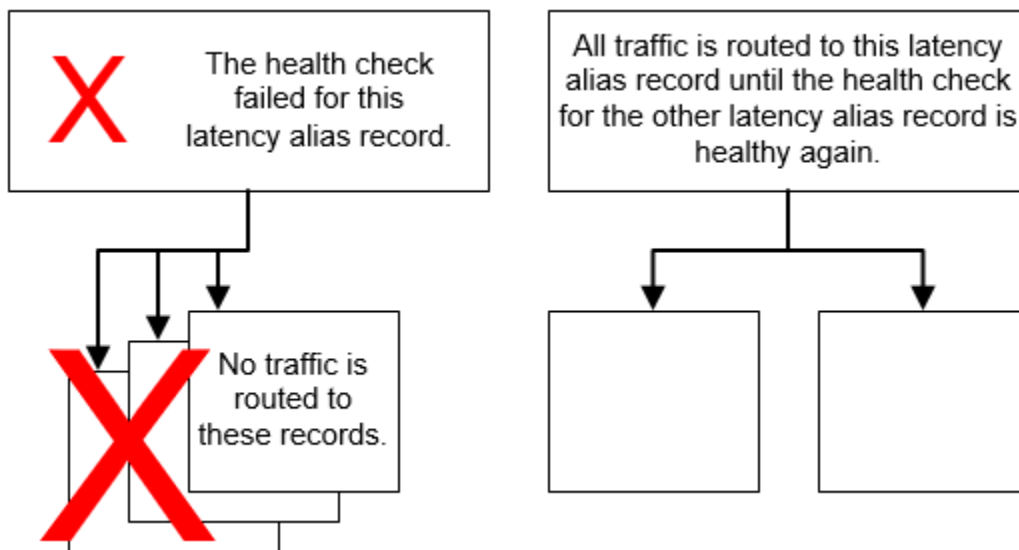
Anda dapat mengaitkan pemeriksaan kondisi dengan catatan alias alih-alih atau sebagai tambahan pengaturan nilai Evaluasi Kondisi Target ke Ya. Namun, umumnya lebih berguna jika Route 53 merespons kueri berdasarkan kondisi sumber daya yang mendasarinya—server HTTP, server basis data, dan sumber daya lain yang dirujuk catatan alias Anda. Sebagai contoh, perhatikan konfigurasi berikut:

- Anda menetapkan pemeriksaan kondisi ke catatan alias latensi di mana target alias adalah grup catatan tertimbang.
- Anda mengatur nilai Evaluasi Kondisi Target ke Ya untuk catatan alias latensi.

Dalam konfigurasi ini, kedua hal berikut harus benar sebelum Route 53 mengembalikan nilai yang ada untuk catatan tertimbang:

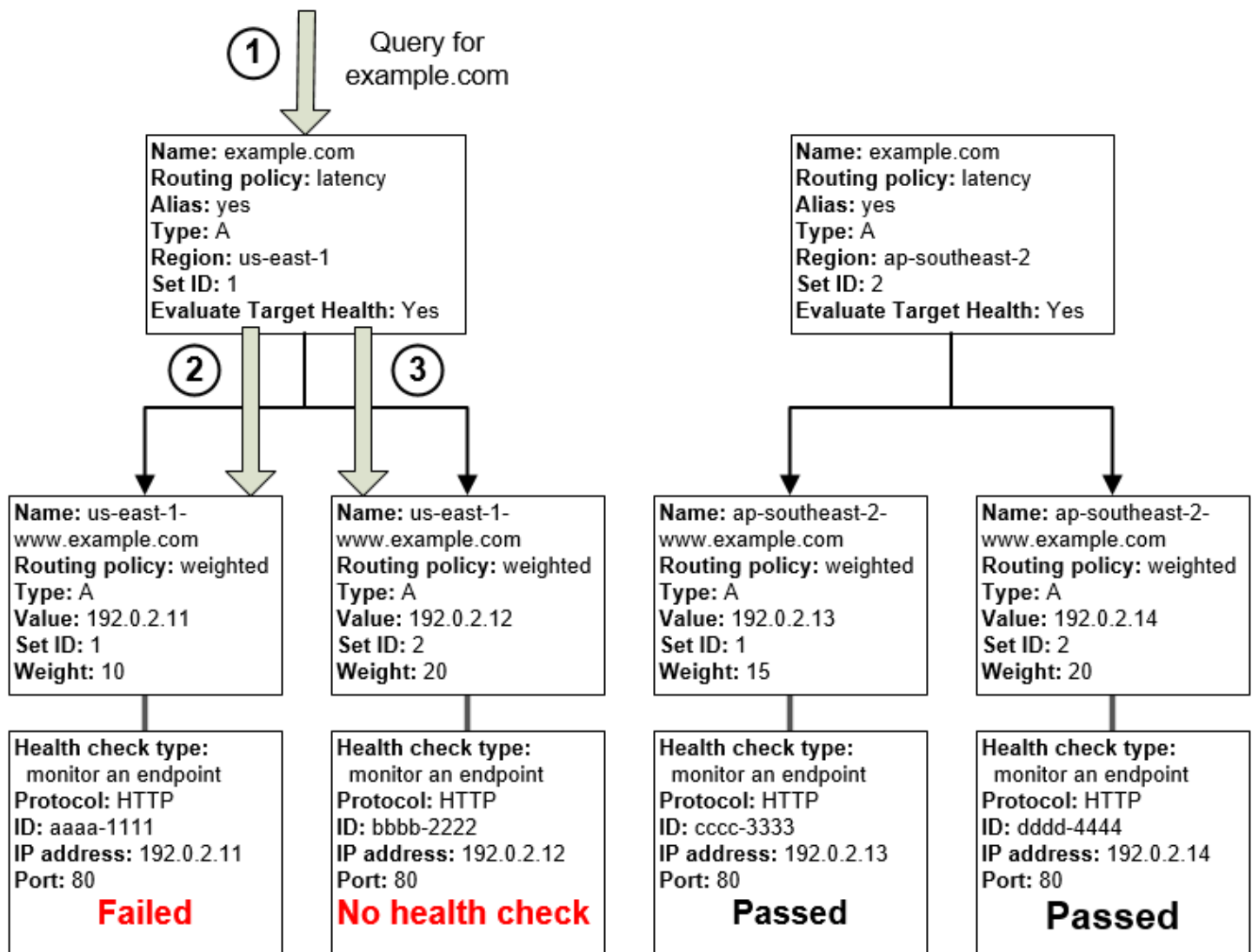
- Harus lolos dari pemeriksaan kondisi yang terkait dengan catatan alias latensi.
- Setidaknya satu catatan tertimbang harus dianggap sehat, baik karena terkait dengan pemeriksaan kondisi yang lolos atau karena tidak terkait dengan pemeriksaan kondisi. Dalam kasus terakhir, Route 53 selalu menganggap catatan tertimbang dalam kondisi sehat.

Dalam ilustrasi berikut, pemeriksaan kondisi untuk catatan alias latensi di kiri atas gagal. Akibatnya, Route 53 berhenti merespons kueri menggunakan salah satu catatan tertimbang yang dirujuk catatan alias latensi, bahkan jika semuanya sehat. Route 53 mulai mempertimbangkan lagi catatan tertimbang ini hanya ketika pemeriksaan kondisi untuk catatan alias latensi kembali sehat. (Untuk pengecualian, lihat [Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi](#).)



Apa yang terjadi jika Anda menghilangkan pemeriksaan kondisi?

Dalam konfigurasi yang kompleks, penting untuk mengaitkan pemeriksaan kondisi dengan semua catatan non-alias. Pada contoh berikut, pemeriksaan kondisi hilang di salah satu catatan tertimbang dalam wilayah us-east-1.



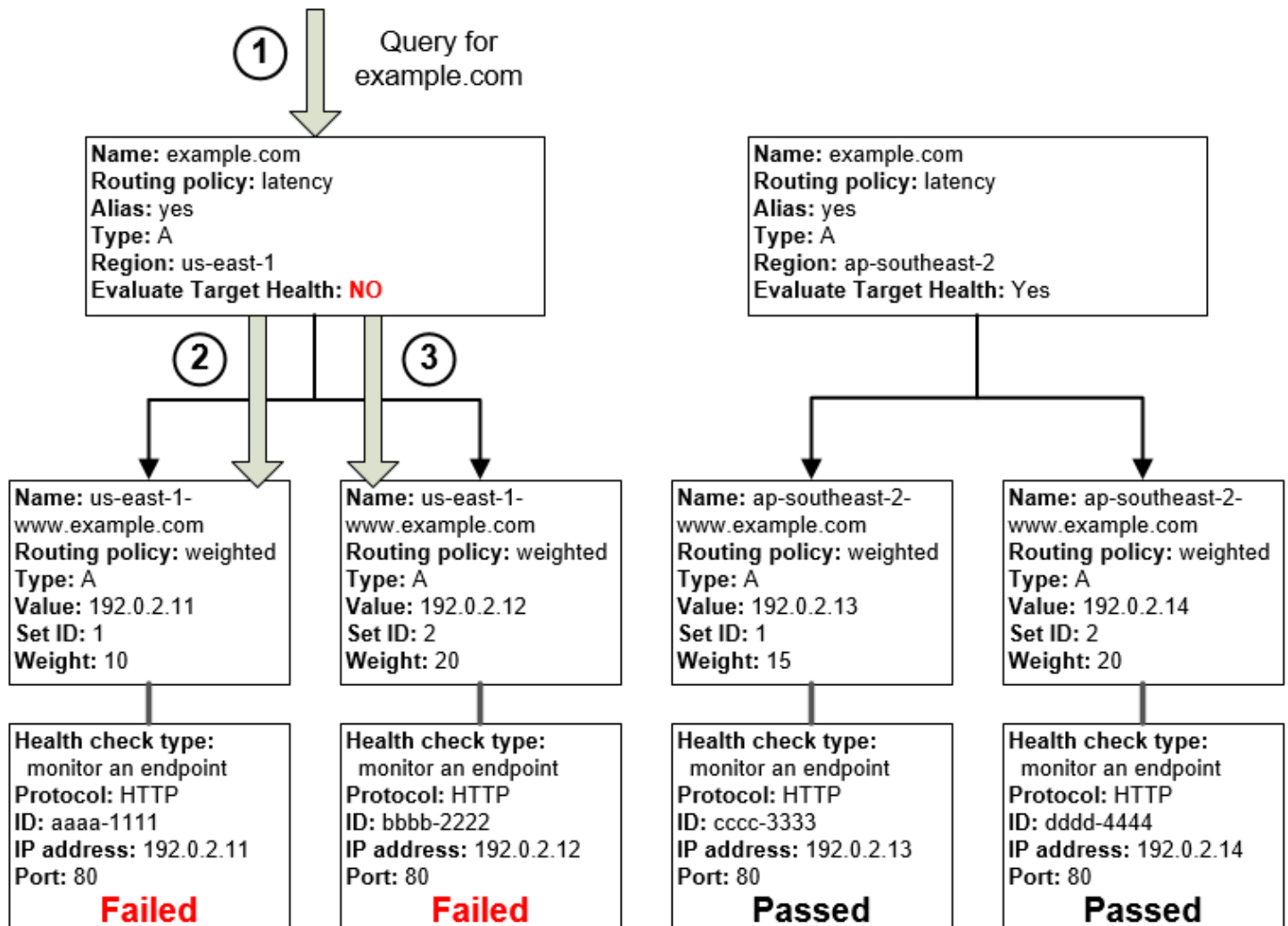
Inilah yang terjadi jika Anda menghilangkan pemeriksaan kondisi pada catatan non-alias dalam konfigurasi ini:

1. Route 53 menerima kueri untuk example.com. Berdasarkan latensi untuk pengguna yang membuat permintaan, Route 53 memilih catatan alias latensi untuk wilayah us-east-1.
2. Route 53 mencari target alias untuk catatan alias latensi, dan memeriksa status pemeriksaan kondisi yang sesuai. Pemeriksaan kondisi untuk satu catatan tertimbang gagal, sehingga catatan dihilangkan dari pertimbangan.
3. Catatan tertimbang lainnya dalam target alias untuk wilayah us-east-1 tidak memiliki pemeriksaan kondisi. Sumber daya yang sesuai mungkin atau mungkin tidak sehat, tapi tanpa pemeriksaan kondisi, Route 53 tidak memiliki cara untuk mengetahuinya. Route 53 menganggap sumber daya ini sehat dan mengembalikan nilai yang ada untuk merespons kueri.

Apa yang terjadi ketika Anda mengatur evaluasi target kondisi ke Tidak?

Secara umum, Anda harus mengatur Evaluasi Kondisi Target ke Ya untuk semua catatan alias pada pohon. Jika Anda menetapkan Evaluate Target Health ke No, Route 53 terus merutekan lalu lintas ke catatan yang dirujuk oleh catatan alias meskipun pemeriksaan kesehatan untuk catatan tersebut gagal.

Pada contoh berikut, semua catatan tertimbang memiliki pemeriksaan kondisi terkait, namun Evaluasi Kondisi Target diatur ke Tidak untuk catatan alias latensi bagi wilayah us-east-1:



Inilah yang terjadi jika Anda mengatur Evaluasi Kondisi Target ke Tidak untuk catatan alias dalam konfigurasi ini:

1. Route 53 menerima kueri untuk example.com. Berdasarkan latensi untuk pengguna yang membuat permintaan, Route 53 memilih catatan alias latensi untuk wilayah us-east-1.

2. Route 53 menentukan target alias untuk catatan alias latensi, dan memeriksa pemeriksaan kondisi yang sesuai. Keduanya gagal.
3. Karena nilai Evaluasi Kondisi Target adalah Tidak untuk catatan alias latensi bagi wilayah us-east-1, Route 53 harus memilih satu catatan di cabang ini alih-alih keluar dari cabang dan mencari catatan yang sehat di wilayah ap-southeast-2.

Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi

Jika Anda mengonfigurasi pemeriksaan kondisi untuk semua catatan dalam grup catatan yang memiliki nama yang sama, jenis yang sama (seperti A atau AAAA), dan kebijakan perutean yang sama (seperti tertimbang atau failover), Route 53 merespons kueri DNS dengan memilih catatan yang sehat dan mengembalikan nilai yang ada dari catatan tersebut.

Misalnya, anggap Anda membuat tiga catatan tertimbang A, dan menetapkan pemeriksaan kondisi untuk ketiganya. Jika pemeriksaan kondisi untuk salah satu catatan tidak sehat, Route 53 merespons kueri DNS dengan alamat IP di salah satu dari dua catatan lainnya.

Berikut adalah cara Route 53 memilih catatan yang sehat:

1. Route 53 awalnya memilih catatan berdasarkan kebijakan perutean dan nilai yang Anda tentukan untuk setiap catatan. Misalnya, untuk catatan tertimbang, Route 53 memilih catatan berdasarkan bobot yang Anda tentukan untuk setiap catatan.
2. Route 53 menentukan apakah catatan sehat:
 - Catatan non-alias dengan pemeriksaan kondisi terkait— Jika Anda mengaitkan pemeriksaan kondisi dengan catatan non-alias, Route 53 memeriksa status pemeriksaan kondisi saat ini.

Route 53 secara berkala memeriksa kondisi titik akhir yang ditentukan dalam pemeriksaan kondisi; layanan ini tidak melakukan pemeriksaan kondisi ketika kueri DNS tiba.

Anda dapat mengaitkan pemeriksaan kondisi dengan catatan alias, namun sebaiknya kaitkan pemeriksaan kondisi hanya dengan catatan non-alias. Untuk informasi selengkapnya, lihat [Apa yang terjadi jika Anda mengaitkan pemeriksaan kondisi dengan catatan alias?](#).

- Catatan alias dengan Evaluasi Kondisi Target diatur ke Ya— Route 53 memeriksa status kondisi sumber daya yang dirujuk catatan alias, misalnya, penyeimbang beban ELB atau catatan lain di zona yang di-hosting yang sama.
3. Jika catatan yang sehat, Route 53 merespons kueri dengan nilai yang ada, seperti alamat IP.

Jika catatan tidak sehat, Route 53 memilih catatan lain menggunakan kriteria yang sama dan mengulangi proses hingga menemukan catatan yang sehat.

Route 53 menggunakan kriteria berikut ketika memilih catatan:

Catatan tanpa pemeriksaan kondisi artinya catatan selalu sehat

Jika catatan dalam grup catatan yang memiliki nama dan jenis yang sama tidak memiliki pemeriksaan kondisi terkait, Route 53 selalu menganggapnya sehat dan selalu menyertakannya di antara kemungkinan respons untuk kueri.

Jika tidak ada catatan yang sehat, semua catatan dianggap sehat

Jika tidak ada catatan yang sehat dalam grup catatan, Route 53 perlu mengembalikan sesuatu untuk merespons kueri DNS, tetapi layanan tidak memiliki dasar untuk memilih salah satu catatan. Dalam keadaan ini, Route 53 menganggap semua catatan dalam grup dalam kondisi sehat dan memilih satu berdasarkan kebijakan perutean dan nilai yang Anda tentukan untuk setiap catatan.

Catatan tertimbang yang memiliki bobot 0

Jika Anda menambahkan pemeriksaan kondisi ke semua catatan dalam grup catatan tertimbang, tetapi Anda memberikan bobot non-nol ke beberapa catatan dan bobot nol untuk catatan lainnya, pemeriksaan kondisi bekerja seperti ketika semua catatan memiliki bobot non-nol dengan pengecualian berikut:

- Route 53 awalnya hanya mempertimbangkan catatan tertimbang non-nol, jika ada.
- Jika semua catatan yang memiliki bobot lebih besar dari 0 dalam kondisi tidak sehat, Route 53 mempertimbangkan catatan tertimbang nol.

Karena Route 53 akan mempertimbangkan catatan berbobot nol dalam beberapa keadaan, penting untuk memastikan bahwa target bobot nol juga memiliki jawaban yang layak untuk kueri DNS.

Untuk informasi selengkapnya tentang catatan tertimbang, lihat [Pemeriksaan kesehatan dan perutean tertimbang](#).

Catatan alias

Anda juga dapat mengonfigurasi pemeriksaan kondisi untuk catatan alias dengan mengatur Evaluasi Kondisi Target ke Ya untuk setiap catatan alias. Hal ini menyebabkan Route 53 mengevaluasi kondisi sumber daya yang menjadi tujuan lalu lintas saat dirutekan oleh catatan, misalnya, penyeimbang beban ELB atau catatan lain di zona yang di-hosting yang sama.

Misalnya, target alias untuk catatan alias adalah grup catatan tertimbang bahwa semuanya memiliki bobot non-nol:

- Selama setidaknya salah satu catatan tertimbang dalam kondisi sehat, Route 53 menganggap catatan alias sehat.
- Jika tidak ada catatan tertimbang dalam kondisi sehat, Route 53 menganggap catatan alias tidak sehat.
- Route 53 berhenti mempertimbangkan catatan di cabang pohon hingga setidaknya satu catatan tertimbang menjadi sehat lagi.

Untuk informasi selengkapnya, lihat [Cara kerja pemeriksaan kondisi dalam konfigurasi Amazon Route 53 yang kompleks](#).

Catatan failover

Catatan failover umumnya bekerja dengan cara yang sama seperti jenis perutean lainnya. Anda membuat pemeriksaan kondisi dan mengaitkannya dengan catatan non-alias, dan Anda mengatur Evaluasi Kondisi Target ke Ya untuk catatan alias. Perhatikan hal berikut:

- Catatan primer dan sekunder dapat menjadi catatan non-alias atau catatan alias.
- Jika Anda mengaitkan pemeriksaan kondisi dengan data failover primer dan sekunder, berikut adalah cara Route 53 merespons permintaan:
 - Jika Route 53 menganggap catatan utama sehat (jika titik akhir pemeriksaan kondisi sehat), Route 53 hanya mengembalikan catatan primer untuk merespons kueri DNS.
 - Jika Route 53 menganggap catatan primer tidak sehat dan catatan sekunder sehat, Route 53 akan mengembalikan catatan sekunder.
 - Jika Route 53 menganggap catatan primer dan catatan sekunder tidak sehat, Route 53 akan mengembalikan catatan primer.
- Jika Anda mengonfigurasi catatan sekunder, penambahan pemeriksaan kondisi bersifat opsional. Jika Anda menghilangkan pemeriksaan kondisi untuk catatan sekunder, dan jika titik akhir pemeriksaan kondisi untuk catatan primer tidak sehat, Route 53 selalu merespons kueri DNS menggunakan catatan sekunder. Inilah yang terjadi bahkan jika catatan sekunder tidak sehat.

Untuk informasi selengkapnya, lihat topik berikut.

- [Mengonfigurasi failover active-passive dengan satu sumber daya primer dan satu sumber daya sekunder](#)
- [Mengonfigurasi failover active-passive dengan beberapa sumber daya primer dan sekunder](#)

Failover active-active dan active-passive

Anda dapat menggunakan pemeriksaan kondisi Route 53 untuk mengonfigurasi konfigurasi failover active-active dan active-passive. Anda mengonfigurasi failover active-active menggunakan semua [kebijakan perutean](#) (atau kombinasi dari kebijakan perutean) selain failover, dan Anda mengonfigurasi failover active-passive menggunakan kebijakan perutean failover.

Topik

- [Failover active-active](#)
- [Failover active-passive](#)

Failover active-active

Gunakan konfigurasi failover ini ketika Anda ingin semua sumber daya tersedia hampir sepanjang waktu. Ketika sumber daya menjadi tidak tersedia, Route 53 dapat mendeteksi bahwa sumber daya tidak sehat dan berhenti menyertakannya saat merespons kueri.

Dalam failover active-active, semua catatan dengan nama yang sama, jenis yang sama (seperti A atau AAAA), dan kebijakan perutean yang sama (seperti tertimbang atau latensi) akan aktif kecuali Route 53 menganggap catatan tidak sehat. Route 53 dapat merespons kueri DNS menggunakan catatan sehat.

Failover active-passive

Gunakan konfigurasi failover active-passive ketika Anda ingin sumber daya atau grup sumber daya primer tersedia hampir sepanjang waktu dan Anda ingin sumber daya atau grup sumber daya sekunder berada dalam kondisi siaga jika semua sumber daya primer tidak tersedia. Ketika merespons kueri, Route 53 hanya menyertakan sumber daya primer yang sehat. Jika semua sumber daya primer tidak sehat, Route 53 mulai hanya menyertakan sumber daya sekunder sehat untuk merespons kueri DNS.

Topik

- [Mengonfigurasi failover active-passive dengan satu sumber daya primer dan satu sumber daya sekunder](#)
- [Mengonfigurasi failover active-passive dengan beberapa sumber daya primer dan sekunder](#)
- [Mengonfigurasi failover active-passive dengan catatan tertimbang](#)

Mengonfigurasi failover active-passive dengan satu sumber daya primer dan satu sumber daya sekunder

Untuk membuat konfigurasi failover active-passive dengan satu catatan primer dan satu catatan sekunder, Anda cukup membuat catatan dan menentukan Failover untuk kebijakan perutean. Ketika sumber daya primer sehat, Route 53 merespons kueri DNS menggunakan catatan primer. Ketika sumber daya primer tidak sehat, Route 53 merespons kueri DNS menggunakan catatan sekunder.

Mengonfigurasi failover active-passive dengan beberapa sumber daya primer dan sekunder

Anda juga dapat mengaitkan beberapa sumber daya dengan catatan primer, catatan sekunder, atau keduanya. Dalam konfigurasi ini, Route 53 menganggap catatan failover primer dalam kondisi sehat selama setidaknya salah satu sumber daya terkait dalam kondisi sehat. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 memilih catatan ketika pemeriksaan kondisi dikonfigurasi](#).

Untuk mengonfigurasi failover active-passive dengan beberapa sumber daya untuk catatan primer atau sekunder, lakukan tugas berikut.

1. Buat pemeriksaan kesehatan untuk setiap sumber daya yang ingin Anda rutekan lalu lintas, seperti EC2 instance atau server web di pusat data Anda.

Note

Jika Anda merutekan lalu lintas ke AWS sumber daya apa pun yang dapat Anda buat [catatan alias](#), jangan membuat pemeriksaan kesehatan untuk sumber daya tersebut. Bila membuat catatan alias, Anda mengatur Evaluasi Kondisi Target ke Ya.

Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

2. Buat catatan untuk sumber daya primer Anda, dan tentukan nilai berikut:
 - Berikan nama, jenis, dan kebijakan perutean yang sama ke setiap catatan. Misalnya, Anda mungkin membuat tiga catatan tertimbang A yang semuanya bernama failover-primary.example.com.
 - Jika Anda menggunakan AWS sumber daya yang dapat Anda buat catatan alias, tentukan Ya untuk Evaluasi Kesehatan Target.

Jika Anda menggunakan sumber daya yang catatan aliasnya tidak dapat Anda buat, kaitkan pemeriksaan kondisi yang ada dari langkah 1 dengan setiap catatan.

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

3. Buat catatan untuk sumber daya sekunder Anda, dan jika ada, tentukan nilai berikut:

- Berikan nama, jenis, dan kebijakan perutean yang sama ke setiap catatan. Misalnya, Anda mungkin membuat tiga catatan tertimbang A yang semuanya bernama failover-secondary.example.com.
- Jika Anda menggunakan AWS sumber daya yang dapat Anda buat catatan alias, tentukan Ya untuk Evaluasi Kesehatan Target.

Jika Anda menggunakan sumber daya yang catatan aliasnya tidak dapat Anda buat, kaitkan pemeriksaan kondisi yang ada dari langkah 1 dengan setiap catatan.

 Note

Beberapa pelanggan menggunakan server web sebagai sumber daya primer mereka dan bucket Amazon S3 yang dikonfigurasi menjadi titik akhir situs web sebagai sumber daya sekunder mereka. Bucket S3 berisi pesan sederhana "sementara tidak tersedia". Jika menggunakan konfigurasi tersebut, Anda dapat melewati langkah ini dan hanya membuat catatan alias failover untuk sumber daya sekunder di langkah 4.

4. Buat dua catatan alias failover, satu primer dan satu sekunder, lalu tentukan nilai berikut:

Catatan primer

- Nama - Tentukan nama domain (example.com) atau nama subdomain (www.example.com) yang Anda inginkan Route 53 untuk merutekan lalu lintas.
- Alias – Atur ke Ya.
- Target Alias – Tentukan nama catatan yang Anda buat di langkah 2.
- Kebijakan Perutean – Atur ke Failover.
- Jenis Catatan Failover – Atur ke Primer.
- Evaluasi Kondisi Target – Atur ke Ya.
- Mengaitkan dengan Pemeriksaan Kondisi – Atur ke Tidak.

Catatan sekunder

- Nama – Tentukan nama yang sama seperti yang Anda tentukan untuk catatan primer.
- Alias – Atur ke Ya.

- Target Alias – Jika Anda membuat catatan untuk sumber daya sekunder di langkah 3, tentukan nama catatan. Jika Anda menggunakan bucket Amazon S3 untuk sumber daya sekunder, tentukan nama DNS dari titik akhir situs web.
- Kebijakan Perutean – Atur ke Failover.
- Jenis Catatan Failover – Atur ke Sekunder.
- Evaluasi Kondisi Target – Atur ke Ya.
- Mengaitkan dengan Pemeriksaan Kondisi – Atur ke Tidak.

Mengonfigurasi failover active-passive dengan catatan tertimbang

Anda juga dapat menggunakan catatan tertimbang untuk failover active-passive, dengan peringatan. Jika Anda menentukan bobot non-nol untuk beberapa catatan dan bobot nol untuk catatan lainnya, Route 53 merespons kueri DNS hanya menggunakan catatan sehat yang memiliki bobot non-nol. Jika semua catatan yang memiliki bobot lebih besar dari 0 dalam kondisi tidak sehat, Route 53 merespons kueri menggunakan catatan tertimbang nol.

Note

Semua catatan dengan bobot non-nol harus tidak sehat sebelum Route 53 mulai merespons kueri DNS menggunakan catatan yang memiliki bobot nol. Tindakan ini dapat membuat aplikasi web atau situs web Anda tidak dapat diandalkan jika sumber daya sehat terakhir, seperti server web, tidak dapat menangani semua lalu lintas ketika sumber daya lain tidak tersedia.

Mengonfigurasi failover di zona yang di-hosting secara privat

Jika Anda membuat catatan failover di zona yang di-hosting secara privat, perhatikan hal berikut:

- Periksa kondisi Route 53 berada di luar VPC. Untuk memeriksa kesehatan titik akhir dalam VPC berdasarkan alamat IP, Anda harus menetapkan alamat IP publik untuk instans di VPC.
- Anda dapat membuat CloudWatch metrik, mengaitkan alarm dengan metrik, dan kemudian membuat pemeriksaan kesehatan yang didasarkan pada aliran data untuk alarm. Misalnya, Anda dapat membuat CloudWatch metrik yang memeriksa status EC2 StatusCheckFailed metrik, menambahkan alarm ke metrik, dan kemudian membuat pemeriksaan kesehatan yang didasarkan pada aliran data untuk alarm untuk memeriksa instance dalam Virtual Private Cloud (VPC) yang

hanya memiliki alamat IP pribadi. Untuk informasi tentang membuat CloudWatch metrik dan alarm menggunakan CloudWatch konsol, lihat [CloudWatch Panduan Pengguna Amazon](#).

Untuk informasi selengkapnya, silakan lihat [Bekerja dengan zona yang di-hosting privat](#) dan [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

Cara Amazon Route 53 mencegah masalah failover

Algoritma failover yang diterapkan oleh Route 53 dirancang tidak hanya untuk mengarahkan lalu lintas ke titik akhir yang sehat, tetapi juga untuk menghindari membuat skenario bencana lebih buruk karena pemeriksaan kesehatan dan aplikasi yang salah konfigurasi, kelebihan titik akhir, dan kegagalan partisi.

Topik

- [Cara Amazon Route 53 mencegah kegagalan cascading](#)
- [Cara Amazon Route 53 menangani partisi internet](#)

Cara Amazon Route 53 mencegah kegagalan cascading

Sebagai pertahanan pertama terhadap kegagalan cascading, setiap algoritme perutean permintaan (seperti tertimbang dan failover) memiliki mode upaya terakhir. Dalam mode khusus ini, ketika semua catatan dianggap tidak sehat, algoritme Route 53 beralih ke menganggap semua catatan dalam kondisi sehat.

Misalnya, jika semua contoh aplikasi, pada beberapa host, menolak permintaan pemeriksaan kondisi, server DNS Route 53 tetap akan memilih jawaban dan mengembalikannya alih-alih tidak mengembalikan jawaban DNS atau mengembalikan respons NXDOMAIN (domain tidak ada). Aplikasi dapat merespons pengguna tetapi tetap gagal dalam pemeriksaan kondisi, oleh karena itu tindakan ini memberikan beberapa perlindungan terhadap kesalahan konfigurasi.

Demikian pula, jika aplikasi kelebihan beban, dan satu dari tiga titik akhir gagal dalam pemeriksaan kondisi, sehingga dikecualikan dari respons DNS Route 53, Route 53 mendistribusikan respons di antara dua titik akhir yang tersisa. Jika titik akhir yang tersisa tidak mampu menangani beban tambahan dan gagal, Route 53 beralih mendistribusikan permintaan ke ketiga titik akhir.

Cara Amazon Route 53 menangani partisi internet

Meski tidak umum, terkadang ada partisi internet yang cukup parah, yang berarti bahwa wilayah geografis yang besar tidak dapat berkomunikasi dengan satu sama lain melalui internet. Selama partisi ini, lokasi Route 53 mungkin mencapai kesimpulan yang berbeda tentang status kesehatan titik akhir dan mungkin berbeda dari status yang dilaporkan. CloudWatch Pemeriksaan kesehatan Route 53 di setiap AWS Wilayah terus-menerus mengirimkan status pemeriksaan kesehatan ke semua lokasi Route 53. Selama partisi internet, setiap lokasi Route 53 mungkin memiliki akses hanya ke sebagian set status ini, biasanya dari wilayah terdekat.

Misalnya, selama partisi internet yang memengaruhi konektivitas ke dan dari Amerika Selatan, server DNS Route 53 di lokasi South America (São Paulo) Route 53 mungkin memiliki akses yang baik ke titik akhir pemeriksaan kondisi di Wilayah AWS South America (São Paulo), tetapi akses yang buruk ke titik akhir di tempat lain. Pada saat yang sama, Route 53 di US East (Ohio) mungkin memiliki akses yang buruk ke titik akhir pemeriksaan kondisi di Wilayah South America (São Paulo), dan menyimpulkan bahwa catatan yang ada tidak sehat.

Partisi seperti ini dapat menimbulkan situasi di mana lokasi Route 53 membuat kesimpulan yang berbeda tentang status kondisi titik akhir, berdasarkan, visibilitas lokal mereka dari titik akhir tersebut. Inilah sebabnya setiap lokasi Route 53 menganggap bahwa titik akhir sehat hanya ketika dianggap sehat oleh sebagian pemeriksa kondisi yang dapat dijangkau.

Penamaan dan penandaan pemeriksaan kondisi

Anda dapat menambahkan tanda ke pemeriksaan kondisi Amazon Route 53, yang memungkinkan Anda memberikan setiap nama yang lebih mudah dipahami ke pemeriksaan kondisi dibandingkan ID pemeriksaan kondisi. Ini adalah tag yang sama yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Gunakan tanda alokasi biaya untuk laporan tagihan kustom](#) dalam Panduan Pengguna AWS Billing .

Setiap tanda terdiri dari sebuah kunci (nama tanda) dan nilai, Anda yang menentukan keduanya. Ketika menambahkan tanda ke pemeriksaan kondisi, kami sarankan Anda menambahkan satu tanda yang memiliki nilai berikut untuk kunci dan nilai:

- kunci – Nama
- nilai – Nama yang ingin Anda berikan ke pemeriksaan kondisi

Nilai tanda Nama muncul dalam daftar pemeriksaan kondisi di konsol Route 53, yang memungkinkan Anda membedakan berbagai pemeriksaan kondisi. Untuk melihat tanda pemeriksaan kondisi lain, pilih pemeriksaan kondisi lalu pilih tab Tanda.

Untuk informasi lebih lanjut tentang tanda, lihat topik berikut:

- Untuk menambahkan, mengedit, atau menghapus tanda Nama saat Anda menambahkan atau mengedit pemeriksaan kondisi di konsol Route 53, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).
- Untuk gambaran umum tentang penandaan sumber daya Route 53, lihat [Memberi tanda pada sumber daya Amazon Route 53](#).

Pembatasan tanda

Batasan dasar berikut berlaku untuk tanda:

- Jumlah maksimum tag per sumber daya — 50 di konsol baru dan 10 di konsol lama.
- Panjang Kunci maksimum – 128 karakter Unicode
- Panjang Nilai maksimum – 256 karakter Unicode
- Nilai yang valid untuk Kunci dan Nilai – huruf besar dan huruf kecil dalam set karakter UTF-8, angka, spasi, serta karakter berikut: `_` `.` `:` `/` `=` `+` `-` dan `@`
- Kunci dan nilai tanda peka huruf besar kecil
- Jangan gunakan `aws:` awalan untuk kunci atau nilai; itu dicadangkan untuk AWS digunakan

Menambahkan, mengedit, dan menghapus tanda untuk pemeriksaan kondisi

Prosedur berikut menunjukkan cara menggunakan tanda untuk pemeriksaan kondisi Anda di konsol Route 53.

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk menambahkan tag ke pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Pilih ID tertaut dari pemeriksaan kesehatan yang ingin Anda tambahkan tag.
4. Di halaman bawah, pilih tab Tag, lalu pilih Kelola dan kemudian Tambahkan tag baru.
5. Masukkan nama untuk tag di bidang Kunci, dan masukkan nilai di bidang Nilai.
6. Pilih Simpan.

Untuk mengedit tag untuk pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Pilih ID yang ditautkan dari pemeriksaan kesehatan.
4. Di panel bawah, pilih tab Tag, lalu pilih Kelola.
5. Anda sekarang dapat mengedit dan menambahkan lebih banyak tag.
6. Pilih Simpan.

Untuk menghapus tag untuk pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Pilih ID yang ditautkan dari pemeriksaan kesehatan.
4. Di panel bawah, pilih tab Tag, lalu pilih Kelola.

5. Pilih Hapus di samping tag yang ingin Anda hapus.
6. Pilih Simpan.

Old console

Untuk menambahkan tag ke pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Pilih pemeriksaan kondisi, atau pilih beberapa pemeriksaan kondisi jika Anda ingin menambahkan tanda yang sama ke lebih dari satu pemeriksaan kondisi.
4. Di panel bawah, pilih tab Tanda, lalu pilih Tambahkan/Edit Tanda.
5. Di kotak dialog Tambahkan/Edit Tanda, masukkan nama untuk tanda di bidang Kunci, dan masukkan nilai di bidang Nilai.
6. Pilih Terapkan perubahan.

Untuk mengedit tag untuk pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Pilih pemeriksaan kondisi.

Jika memilih beberapa pemeriksaan kondisi dengan tanda yang sama, Anda tidak dapat mengedit nilai untuk semua tanda secara bersamaan. Namun, perhatikan bahwa Anda dapat mengedit nilai tanda yang muncul di beberapa pemeriksaan kondisi jika memilih pemeriksaan kondisi yang memiliki tanda dan setidaknya satu yang tidak memiliki tanda.

Misalnya, Anda memilih beberapa pemeriksaan kondisi yang memiliki tanda Pusat Biaya dan satu yang tidak memiliki tanda. Anda memilih opsi untuk menambahkan tanda, dan Anda menentukan Pusat Biaya sebagai kunci dan 777 sebagai nilai. Untuk pemeriksaan kondisi yang dipilih dan sudah memiliki tanda Pusat Biaya, Route 53 mengubah nilainya menjadi 777. Untuk satu pemeriksaan kondisi yang tidak memiliki tanda Pusat Biaya, Route 53 menambahkan satu tanda dan menetapkan nilainya menjadi 777.

4. Di panel bawah, pilih tab Tanda, lalu pilih Tambahkan/Edit Tanda.

5. Di kotak dialog Tambahkan/Edit Tanda, edit nilainya.
6. Pilih Simpan.

Untuk menghapus tag untuk pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Pilih pemeriksaan kondisi, atau pilih beberapa pemeriksaan kondisi jika Anda ingin menghapus tanda yang sama dari lebih dari satu pemeriksaan kondisi.
4. Di panel bawah, pilih tab Tanda, lalu pilih Tambahkan/Edit Tanda.
5. Di kotak dialog Tambah/Edit Tag, pilih di **X** sebelah tag yang ingin Anda hapus.
6. Pilih Simpan.

Menggunakan pemeriksaan kondisi dengan versi API Amazon Route 53 yang lebih awal dari 2012-12-12

Pemeriksaan kondisi didukung mulai dari versi 2012-12-12 API Amazon Route 53. Jika zona yang di-hosting berisi catatan bahwa pemeriksaan kondisi telah dikonfigurasi, kami sarankan Anda hanya menggunakan API 2012-12-12 atau yang lebih baru. Perhatikan batasan berikut saat menggunakan pemeriksaan kondisi dengan versi API sebelumnya.

- Tindakan `ChangeResourceRecordSets` tidak dapat membuat atau menghapus catatan yang menyertakan elemen `EvaluateTargetHealth`, `Failover`, atau `HealthCheckId`.
- Tindakan `ListResourceRecordSets` dapat mencantumkan catatan yang menyertakan elemen tersebut, tetapi elemen tidak disertakan dalam output. Sebagai gantinya, elemen `Value` pada respons berisi pesan yang mengatakan catatan menyertakan atribut yang tidak didukung.

Memantau status pemeriksaan kondisi dan mendapatkan notifikasi

Anda memantau status pemeriksaan kondisi di konsol Amazon Route 53. Anda juga dapat mengatur CloudWatch alarm dan mendapatkan notifikasi otomatis ketika status pemeriksaan kesehatan Anda berubah.

Topik

- [Melihat status pemeriksaan kondisi dan alasan kegagalan pemeriksaan kondisi](#)
- [Memantau latensi antara pemeriksa kondisi dan titik akhir Anda](#)
- [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#)

Melihat status pemeriksaan kondisi dan alasan kegagalan pemeriksaan kondisi

Di konsol Route 53, Anda dapat melihat status (sehat atau tidak sehat) pemeriksaan kondisi seperti yang dilaporkan oleh pemeriksa kondisi Route 53. Untuk semua pemeriksaan kondisi, kecuali pemeriksaan kondisi yang dihitung, Anda juga dapat melihat alasan kegagalan pemeriksaan kondisi terakhir, misalnya, pemeriksa kondisi tidak dapat membuat koneksi dengan titik akhir.

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk melihat status dan alasan kegagalan terakhir untuk pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Untuk gambaran umum semua status pemeriksaan kondisi Anda—sehat atau tidak sehat—lihat kolom Status. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).
4. Untuk semua pemeriksaan kondisi, kecuali pemeriksaan kondisi yang dihitung, Anda dapat melihat status pemeriksa kondisi Route 53 yang memeriksa kondisi titik akhir yang ditentukan.
5. Pilih ID tertaut dari pemeriksaan kesehatan yang ingin Anda lihat detailnya.
6. Di panel bawah, pilih tab Pemeriksa Kesehatan.

Note

Pemeriksaan kondisi baru harus disebarkan ke pemeriksa kondisi Route 53 sebelum status pemeriksaan kondisi dan alasan kegagalan terakhir muncul di kolom Status. Hingga penyebaran selesai, pesan di kolom tersebut menjelaskan bahwa tidak ada status yang tersedia.

7. Tabel ini mencakup nilai-nilai berikut:

IP pemeriksa kondisi

Alamat IP pemeriksa kondisi Route 53 yang melakukan pemeriksaan kondisi.

Terakhir diperiksa

Tanggal dan waktu pemeriksaan kesehatan atau tanggal dan waktu kegagalan terakhir.

Status

Entah status pemeriksaan kesehatan saat ini atau alasan kegagalan pemeriksaan kesehatan terakhir.

Old console

Untuk melihat status dan alasan kegagalan terakhir untuk pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Untuk gambaran umum semua status pemeriksaan kondisi Anda—sehat atau tidak sehat—lihat kolom Status. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).
4. Untuk semua pemeriksaan kondisi, kecuali pemeriksaan kondisi yang dihitung, Anda dapat melihat status pemeriksaan kondisi Route 53 yang memeriksa kondisi titik akhir yang ditentukan. Pilih pemeriksaan kondisi.
5. Di panel bawah, pilih tab Periksa Kondisi .

Note

Pemeriksaan kondisi baru harus disebarkan ke pemeriksa kondisi Route 53 sebelum status pemeriksaan kondisi dan alasan kegagalan terakhir muncul di kolom Status. Hingga penyebaran selesai, pesan di kolom tersebut menjelaskan bahwa tidak ada status yang tersedia.

6. Pilih apakah Anda ingin melihat status pemeriksaan kondisi saat ini, atau melihat tanggal dan waktu kegagalan terakhir serta alasan kegagalan tersebut. Tabel di tab Status mencakup nilai berikut:

IP pemeriksa kondisi

Alamat IP pemeriksa kondisi Route 53 yang melakukan pemeriksaan kondisi.

Terakhir diperiksa

Tanggal dan waktu pemeriksaan kondisi atau tanggal dan waktu kegagalan terakhir, tergantung pada opsi yang Anda pilih di bagian atas tab Status.

Status

Baik status pemeriksaan kondisi saat ini atau alasan kegagalan pemeriksaan kondisi terakhir, tergantung pada opsi yang Anda pilih di bagian atas tab Status.

Memantau latensi antara pemeriksa kondisi dan titik akhir Anda

Saat Anda membuat pemeriksaan kesehatan, jika Anda memilih untuk memantau status titik akhir (bukan status pemeriksaan kesehatan lainnya) dan Anda memilih opsi Grafik latensi, Anda dapat melihat nilai berikut pada CloudWatch grafik di konsol Route 53:

- Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 untuk membuat koneksi TCP dengan titik akhir
- Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 untuk menerima byte pertama respons bagi permintaan HTTP atau HTTPS
- Rata-rata waktu, dalam milidetik, yang dibutuhkan oleh pemeriksa kondisi Route 53 untuk menyelesaikan handshake SSL/TLS

Note

Anda tidak dapat mengaktifkan pemantauan latensi untuk pemeriksaan kondisi yang ada.

Important

Pemeriksa kesehatan dijalankan di 16 zona ketersediaan redundan. Terkadang zona ketersediaan tidak tersedia karena penerapan, pembaruan, pemeliharaan, dan sebagainya. Sistem pemeriksaan kesehatan dirancang untuk menjelaskan hal ini tanpa dampak pelanggan.

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk melihat latensi antara pemeriksa kesehatan Route 53 dan titik akhir Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Pilih ID tertaut untuk pemeriksaan kesehatan yang ingin Anda lihat metriknya. Anda dapat melihat data latensi hanya untuk pemeriksaan kondisi yang memantau status titik akhir dan dengan opsi Grafik latensi yang diaktifkan.
4. Di panel bawah, pilih tab Metrik.
5. Pilih rentang waktu dan wilayah geografis yang ingin Anda tampilkan grafik latensinya.

Grafik menampilkan status untuk rentang waktu yang ditentukan:

Waktu koneksi TCP (hanya HTTP dan TCP)

Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 di wilayah geografis yang dipilih untuk membuat koneksi TCP dengan titik akhir.

Waktu ke byte pertama (hanya HTTP dan HTTPS)

Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 di wilayah geografis yang dipilih untuk menerima byte pertama dari respons bagi permintaan HTTP atau HTTPS.

Waktu untuk menyelesaikan handshake SSL (HTTPS saja)

Rata-rata waktu, dalam milidetik, yang dibutuhkan oleh pemeriksa kondisi Route 53 di wilayah geografis yang dipilih untuk menyelesaikan handshake SSL/TLS.

6. Untuk melihat grafik yang lebih besar dan menentukan pengaturan yang berbeda, pilih tiga titik di kanan atas grafik. Anda dapat mengubah pengaturan berikut:

Statistik

Mengubah perhitungan yang CloudWatch dilakukan pada data.

Rentang waktu

Menampilkan status pemeriksaan kondisi selama periode yang berbeda, misalnya semalaman atau minggu lalu.

Periode

Mengubah interval antara titik data dalam grafik.

Perhatikan hal berikut:

- Jika baru saja membuat pemeriksaan kondisi, Anda mungkin perlu menunggu beberapa menit agar data muncul di grafik dan agar metrik pemeriksaan kondisi muncul dalam daftar metrik yang tersedia.
- Grafik tidak menyegarkan diri secara otomatis. Untuk memperbarui tampilan, pilih ikon



).

- Jika pemeriksaan kondisi gagal karena beberapa alasan, seperti waktu koneksi habis, Route 53 tidak dapat mengukur latensi, dan data latensi akan hilang dari grafik untuk periode yang terpengaruh.

Old console

Untuk melihat latensi antara pemeriksa kesehatan Route 53 dan titik akhir Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Pilih baris untuk pemeriksaan kondisi yang ada. Anda dapat melihat data latensi hanya untuk pemeriksaan kondisi yang memantau status titik akhir dan dengan opsi Grafik latensi yang diaktifkan.
4. Pada panel bawah, pilih tab Latensi.
5. Pilih rentang waktu dan wilayah geografis yang ingin Anda tampilkan grafik latensinya.

Grafik menampilkan status untuk rentang waktu yang ditentukan:

Waktu koneksi TCP (hanya HTTP dan TCP)

Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 di wilayah geografis yang dipilih untuk membuat koneksi TCP dengan titik akhir.

Waktu ke byte pertama (hanya HTTP dan HTTPS)

Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 di wilayah geografis yang dipilih untuk menerima byte pertama dari respons bagi permintaan HTTP atau HTTPS.

Waktu untuk menyelesaikan handshake SSL (HTTPS saja)

Rata-rata waktu, dalam milidetik, yang dibutuhkan oleh pemeriksa kondisi Route 53 di wilayah geografis yang dipilih untuk menyelesaikan handshake SSL/TLS.

Note

Jika Anda memilih lebih dari satu pemeriksaan kondisi, grafik menampilkan baris kode warna terpisah untuk setiap pemeriksaan kondisi.

6. Untuk melihat grafik yang lebih besar dan menentukan pengaturan yang berbeda, klik grafik. Anda dapat mengubah pengaturan berikut:

Statistik

Mengubah perhitungan yang CloudWatch dilakukan pada data.

Rentang waktu

Menampilkan status pemeriksaan kondisi selama periode yang berbeda, misalnya semalaman atau minggu lalu.

Periode

Mengubah interval antara titik data dalam grafik.

Perhatikan hal berikut:

- Jika baru saja membuat pemeriksaan kondisi, Anda mungkin perlu menunggu beberapa menit agar data muncul di grafik dan agar metrik pemeriksaan kondisi muncul dalam daftar metrik yang tersedia.
- Grafik tidak menyegarkan diri secara otomatis. Untuk memperbarui tampilan, pilih ikon



).

- Jika pemeriksaan kondisi gagal karena beberapa alasan, seperti waktu koneksi habis, Route 53 tidak dapat mengukur latensi, dan data latensi akan hilang dari grafik untuk periode yang terpengaruh.

Memantau pemeriksaan kesehatan menggunakan CloudWatch

Pemeriksaan kesehatan Route 53 terintegrasi dengan CloudWatch metrik sehingga Anda dapat melakukan hal berikut:

- Memverifikasi apakah pemeriksaan kondisi dikonfigurasi dengan benar.
- Meninjau status pemeriksaan kondisi selama jangka waktu tertentu.
- Konfigurasi CloudWatch untuk mengirim peringatan Amazon SNS saat status pemeriksaan kesehatan tidak sehat. Perhatikan bahwa beberapa menit mungkin berlalu antara waktu pemeriksaan kondisi gagal dan waktu ketika Anda menerima notifikasi SNS terkait.

Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Topik

- [Lihat status pemeriksaan kesehatan Anda](#)
- [Lihat alarm pemeriksaan kesehatan](#)
- [Lihat metrik pemeriksaan kesehatan di konsol CloudWatch](#)
- [Buat alarm dengan notifikasi SNS](#)

Lihat status pemeriksaan kesehatan Anda

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)

- [Konsol lama](#)

New console

Untuk melihat status pemeriksaan kesehatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kesehatan.
3. Pilih ID tertaut dari pemeriksaan kesehatan yang ingin Anda lihat metriknya.
4. Di panel bawah, pilih tab Metrik.

Dua grafik menampilkan status jam-jam terakhir dalam interval satu menit:

Status pemeriksaan kesehatan

Grafik menunjukkan penilaian kondisi titik akhir Route 53. 1 berarti sehat dan 0 berarti tidak sehat.

Pemeriksa kesehatan yang melaporkan titik akhir sehat (%)

Untuk pemeriksaan kondisi yang hanya memantau titik akhir, grafik menunjukkan persentase pemeriksaan kondisi Route 53 yang menganggap titik akhir yang dipilih dalam kondisi sehat.

Bila pemeriksaan kondisi dinonaktifkan, metrik ini tidak tersedia.

Jumlah pemeriksaan kesehatan anak yang sehat

Untuk pemeriksaan kondisi yang dihitung saja, grafik menunjukkan jumlah pemeriksaan kondisi anak yang sehat.

5. Untuk melihat grafik yang lebih besar dan menentukan pengaturan yang berbeda, pilih tiga titik di kanan atas, lalu Perbesar. Anda dapat mengubah pengaturan berikut:

Statistik

Mengubah perhitungan yang CloudWatch dilakukan pada data.

Rentang waktu

Menampilkan status pemeriksaan kondisi selama periode yang berbeda, misalnya semalaman atau minggu lalu.

Periode

Mengubah interval antara titik data dalam grafik.

Perhatikan hal berikut:

- Jika baru saja membuat pemeriksaan kondisi, Anda mungkin perlu menunggu beberapa menit agar data muncul di grafik dan agar metrik pemeriksaan kondisi muncul dalam daftar metrik yang tersedia.
- Grafik tidak menyegarkan diri secara otomatis. Untuk memperbarui tampilan, pilih ikon



).

Old console

Untuk melihat status pemeriksaan kesehatan (konsol baru)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pemeriksaan Kondisi.
3. Pilih baris untuk pemeriksaan kondisi yang ada.
4. Pada panel bawah, pilih tab Pemantauan.

Dua grafik menampilkan status jam-jam terakhir dalam interval satu menit:

Status pemeriksaan kesehatan

Grafik menunjukkan penilaian kondisi titik akhir Route 53. 1 berarti sehat dan 0 berarti tidak sehat.

Pemeriksa kesehatan yang melaporkan titik akhir sehat (%)

Untuk pemeriksaan kondisi yang hanya memantau titik akhir, grafik menunjukkan persentase pemeriksaan kondisi Route 53 yang menganggap titik akhir yang dipilih dalam kondisi sehat.

Bila pemeriksaan kondisi dinonaktifkan, metrik ini tidak tersedia.

Jumlah pemeriksaan kesehatan anak yang sehat

Untuk pemeriksaan kondisi yang dihitung saja, grafik menunjukkan jumlah pemeriksaan kondisi anak yang sehat.

Note

Jika Anda memilih lebih dari satu pemeriksaan kondisi, grafik menampilkan baris kode warna terpisah untuk setiap pemeriksaan kondisi.

5. Untuk melihat grafik yang lebih besar dan menentukan pengaturan yang berbeda, klik grafik. Anda dapat mengubah pengaturan berikut:

Statistik

Mengubah perhitungan yang CloudWatch dilakukan pada data.

Rentang waktu

Menampilkan status pemeriksaan kondisi selama periode yang berbeda, misalnya semalaman atau minggu lalu.

Periode

Mengubah interval antara titik data dalam grafik.

Perhatikan hal berikut:

- Jika baru saja membuat pemeriksaan kondisi, Anda mungkin perlu menunggu beberapa menit agar data muncul di grafik dan agar metrik pemeriksaan kondisi muncul dalam daftar metrik yang tersedia.

- Grafik tidak menyegarkan diri secara otomatis. Untuk memperbarui tampilan, pilih ikon segarkan



).

Lihat alarm pemeriksaan kesehatan

Note

Kami memperbarui konsol pemeriksaan kesehatan untuk Route 53. Selama masa transisi, Anda dapat terus menggunakan konsol lama.

Pilih tab untuk konsol yang Anda gunakan.

- [Konsol baru](#)
- [Konsol lama](#)

New console

Untuk melihat status CloudWatch alarm dan mengedit alarm untuk Amazon Route 53

1. Di panel navigasi konsol Route 53, pilih Pemeriksaan Kesehatan.
2. Pilih ID yang ditautkan dari pemeriksaan kesehatan yang ingin Anda lihat alarmnya.
3. Di halaman detail, di bagian bawah halaman, pilih tab Alarm.

Daftar Alarm berisi semua alarm Route 53 yang telah Anda buat untuk pemeriksaan kesehatan yang dipilih.

Kolom Status menunjukkan status saat ini dari setiap alarm:

OK

CloudWatch telah mengumpulkan statistik yang cukup dari pemeriksaan kesehatan Route 53 untuk menentukan bahwa titik akhir tidak memenuhi ambang alarm.

DATA TIDAK MENCIKUP

CloudWatch belum mengumpulkan statistik yang cukup untuk menentukan apakah titik akhir memenuhi ambang alarm. Ini adalah status awal alarm baru. Status alarm juga

berubah menjadi DATA TIDAK MENCIKUPI jika CloudWatch metrik menjadi tidak tersedia atau jika Anda menghapus pemeriksaan kesehatan tanpa menghapus alarm terkait.

ALARM

CloudWatch telah mengumpulkan statistik yang cukup dari pemeriksaan kesehatan Route 53 untuk menentukan bahwa titik akhir memenuhi ambang alarm dan mengirim pemberitahuan ke alamat email yang ditentukan.

4. Untuk melihat alarm di CloudWatch konsol, yang memberikan informasi lebih rinci tentang alarm (misalnya, riwayat pembaruan alarm dan perubahan status), pilih nama alarm yang ditautkan. Anda juga dapat mengedit alarm di CloudWatch konsol.
5. Untuk membuat CloudWatch alarm baru di CloudWatch konsol, pilih Buat CloudWatch alarm. Untuk informasi selengkapnya, lihat [Menemukan dan membuat alarm yang disarankan](#) di Panduan CloudWatch pengguna.

Old console

Untuk melihat status CloudWatch alarm dan mengedit alarm untuk Amazon Route 53

1. Di panel navigasi konsol Route 53, pilih Pemeriksaan Kondisi .
2. Pilih baris untuk pemeriksaan kondisi.
3. Pada panel detail (setelah x Pemeriksaan Kondisi Dipilih), pilih ikon tanda sisipan  yang tepat.

Daftar CloudWatch Alarm berisi semua alarm Route 53 yang telah Anda buat menggunakan akun saat ini AWS .

Kolom Status menunjukkan status saat ini dari setiap alarm:

OK

CloudWatch telah mengumpulkan statistik yang cukup dari pemeriksaan kesehatan Route 53 untuk menentukan bahwa titik akhir tidak memenuhi ambang alarm.

DATA TIDAK MENCIKUPI

CloudWatch belum mengumpulkan statistik yang cukup untuk menentukan apakah titik akhir memenuhi ambang alarm. Ini adalah status awal alarm baru. Status alarm juga

berubah menjadi DATA TIDAK MENCIKUPI jika CloudWatch metrik menjadi tidak tersedia atau jika Anda menghapus pemeriksaan kesehatan tanpa menghapus alarm terkait.

ALARM

CloudWatch telah mengumpulkan statistik yang cukup dari pemeriksaan kesehatan Route 53 untuk menentukan bahwa titik akhir memenuhi ambang alarm dan mengirim pemberitahuan ke alamat email yang ditentukan.

4. Untuk melihat atau mengedit pengaturan alarm, pilih nama alarm.
5. Untuk melihat alarm di CloudWatch konsol, yang memberikan informasi lebih rinci tentang alarm (misalnya, riwayat pembaruan alarm dan perubahan status), pilih Lihat di kolom Opsi Lainnya untuk alarm.
6. Untuk melihat semua CloudWatch alarm yang Anda buat menggunakan AWS akun saat ini, termasuk alarm untuk AWS layanan lain, pilih Lihat Semua CloudWatch Alarm.
7. Untuk melihat semua CloudWatch metrik yang tersedia, termasuk metrik yang saat ini tidak digunakan oleh AWS akun saat ini, pilih Lihat Semua CloudWatch Metrik.

Lihat metrik pemeriksaan kesehatan di konsol CloudWatch

Untuk melihat metrik Route 53 di konsol CloudWatch

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Mengubah wilayah saat ini menjadi US East (N. Virginia). Metrik Route 53 tidak tersedia jika Anda memilih wilayah lain sebagai wilayah saat ini.
3. Di panel navigasi, pilih Metrik.
4. Pada tab Semua metrik, pilih Route 53.
5. Pilih Metrik Pemeriksaan Kondisi.
6. Anda juga dapat mengatur notifikasi SNS di CloudWatch konsol. Untuk informasi selengkapnya, lihat [Membuat alarm yang direkomendasikan](#) di Panduan CloudWatch Pengguna.

Buat alarm dengan notifikasi SNS

Note

Prosedur berikut hanya berlaku untuk konsol lama. Konsol baru mengarahkan Anda ke CloudWatch konsol untuk membuat alarm. Untuk informasi selengkapnya, lihat [Menemukan dan membuat alarm yang disarankan](#) di Panduan CloudWatch pengguna.

Untuk menerima notifikasi Amazon SNS saat status pemeriksaan kesehatan tidak sehat (konsol lama)

1. Di panel navigasi konsol Route 53, pilih Pemeriksaan Kondisi .
2. Pilih baris untuk pemeriksaan kondisi yang ada.
3. Pada panel bawah, pilih tab Alarm.

Tabel mencantumkan alarm yang telah Anda buat untuk pemeriksaan kondisi ini.

4. Pilih Buat Alarm.
5. Tentukan nilai-nilai berikut ini:

Nama alarm

Masukkan nama yang Anda ingin ditampilkan Route 53 pada kolom Nama di tab Alarm.

Deskripsi alarm

(Opsional) Masukkan deskripsi untuk alarm. Nilai ini muncul di CloudWatch konsol.

Kirim notifikasi

Pilih apakah Anda ingin Route 53 mengirimkan notifikasi jika status pemeriksaan kondisi ini memicu alarm.

Target notifikasi (Hanya ketika "Kirim notifikasi" adalah "Ya")

Jika Anda CloudWatch ingin mengirim pemberitahuan ke topik SNS yang ada, pilih topik dari daftar.

Jika Anda CloudWatch ingin mengirim notifikasi tetapi tidak ke topik SNS yang ada, lakukan salah satu hal berikut:

- Jika Anda CloudWatch ingin mengirim pemberitahuan email - Pilih topik SNS Baru dan lanjutkan dengan prosedur ini.
- Jika Anda CloudWatch ingin mengirim notifikasi dengan metode lain — Buka tab browser baru, buka konsol Amazon SNS, dan buat topik baru. Kemudian kembali ke konsol Route 53, pilih nama topik baru dari daftar Target notifikasi, dan lanjutkan prosedur ini.

Nama topik (Hanya ketika Anda memilih untuk membuat topik Amazon SNS baru)

Masukkan nama untuk topik Amazon SNS baru.

Alamat email penerima (Hanya ketika Anda memilih untuk membuat topik Amazon SNS baru)

Masukkan alamat email yang akan dikirim notifikasi SNS oleh Route 53 ketika pemeriksaan kondisi memicu alarm.

Target alarm

Pilih nilai yang ingin dievaluasi oleh Route 53 untuk pemeriksaan kondisi ini:

- Status pemeriksaan kondisi – Periksa kondisi Route 53 melaporkan bahwa pemeriksaan kondisi sehat atau tidak sehat
- Periksa kondisi yang melaporkan titik akhir sehat (%) (pemeriksaan kondisi yang memantau titik akhir saja) – Persentase pemeriksaan kondisi Route 53 yang melaporkan bahwa status pemeriksaan kondisi sehat
- Jumlah pemeriksaan kondisi anak yang sehat (pemeriksaan kondisi yang dihitung saja) – Jumlah pemeriksaan kondisi anak dalam pemeriksaan kondisi yang dihitung yang melaporkan bahwa status pemeriksaan kondisi sehat
- Waktu koneksi TCP (Pemeriksaan kondisi HTTP dan TCP saja) – Waktu dalam milidetik yang dibutuhkan pemeriksaan kondisi Route 53 untuk membuat koneksi TCP dengan titik akhir
- Waktu untuk menyelesaikan handshake SSL (Pemeriksaan kondisi HTTPS saja) – Waktu dalam milidetik yang dibutuhkan pemeriksaan kondisi Route 53 untuk menyelesaikan handshake SSL/TLS
- Waktu ke byte pertama (Pemeriksaan kondisi HTTP dan HTTPS saja) – Waktu dalam milidetik yang dibutuhkan pemeriksaan kondisi Route 53 untuk menerima byte pertama respons bagi permintaan HTTP atau HTTPS

Target alarm

Untuk target alarm yang didasarkan pada latensi (waktu koneksi TCP, Waktu untuk menyelesaikan jabat tangan SSL, Waktu ke byte pertama), pilih apakah Anda ingin menghitung latensi CloudWatch untuk pemeriksaan kesehatan Route 53 di wilayah tertentu atau untuk semua wilayah (Global).

Perhatikan bahwa jika Anda memilih satu wilayah, Route 53 hanya mengukur latensi dua kali per menit, dan jumlah sampel akan lebih kecil dibandingkan jika Anda memilih semua wilayah. Akibatnya, nilai terluar mungkin muncul. Untuk mencegah pemberitahuan alarm palsu, kami sarankan Anda menentukan jumlah periode berturut-turut yang lebih besar bahwa pemeriksaan kesehatan harus gagal sebelum CloudWatch mengirimkan pemberitahuan kepada Anda.

Syarat terpenuhi

Gunakan pengaturan berikut untuk menentukan kapan CloudWatch harus memicu alarm.

Target alarm	Syarat yang direkomendasikan	Deskripsi
Status pemeriksaan kesehatan	Minimum < 1	Pemeriksa kondisi Route 53 melaporkan ketika titik akhir tidak sehat.
Pemeriksa kesehatan yang melaporkan titik akhir sehat (%)	Rata-rata < persentase yang diinginkan	Pemeriksaan kondisi yang hanya memantau titik akhir – Route 53 menganggap status pemeriksaan kondisi sebagai tidak sehat ketika kurang dari 18% dari pemeriksa kondisi melaporkan bahwa statusnya sehat. Jangan pilih Jumlah Sampel untuk metrik ini karena rentang jumlah sampel dapat berubah ketika Route 53 menambahkan lebih banyak wilayah pemeriksaan kondisi. Rata-rata secara akurat akan selalu mewakili persentase pemeriksa yang melaporkan status pemeriksaan kondisi.

Target alarm	Syarat yang direkomendasikan	Deskripsi
Jumlah pemeriksaan kesehatan anak yang sehat	Minimum < jumlah yang diinginkan dari pemeriksaan kondisi anak yang sehat	Statistik Minimum mengembalikan nilai yang paling konservatif dan mewakili skenario terburuk.
Waktu koneksi TCP	Rata-rata > waktu yang diinginkan dalam milidetik	Rata-rata adalah nilai yang lebih konsisten dibandingkan statistik lainnya.
Saatnya menyelesaikan jabat tangan SSL	Rata-rata > waktu yang diinginkan dalam milidetik	Rata-rata adalah nilai yang lebih konsisten dibandingkan statistik lainnya.
Waktu untuk byte pertama	Rata-rata > waktu yang diinginkan dalam milidetik	Rata-rata adalah nilai yang lebih konsisten dibandingkan statistik lainnya.

Setidaknya untuk **x** periode berturut-turut **y** minutes/hours/day

Tentukan berapa banyak periode waktu berturut-turut yang harus dipenuhi oleh nilai-nilai sebelum Route 53 mengirimkan notifikasi. Lalu tentukan durasi periode waktu.

6. Jika Anda memilih Buat, Amazon SNS mengirimkan email dengan informasi tentang topik SNS baru.
7. Di email, pilih Konfirmasi langganan. Anda harus mengonfirmasi langganan Anda untuk mulai menerima CloudWatch pemberitahuan.

Menggunakan DNS Firewall untuk menyaring lalu lintas DNS keluar

Dengan Resolver DNS Firewall, Anda dapat memfilter dan mengatur lalu lintas DNS keluar untuk virtual private cloud (VPC) Anda. Untuk melakukannya, Anda membuat kumpulan aturan pemfilteran yang dapat digunakan kembali di grup aturan DNS Firewall, mengasosiasikan grup aturan ke VPC Anda, lalu memantau aktivitas di log dan metrik DNS Firewall. Berdasarkan aktivitas, Anda dapat menyesuaikan perilaku DNS Firewall.

DNS Firewall memberikan perlindungan untuk permintaan DNS keluar dari Anda. VPCs Permintaan ini dirutekan melalui VPC Resolver untuk resolusi nama domain. Penggunaan utama perlindungan DNS Firewall adalah untuk membantu mencegah eksfiltrasi DNS data Anda. Eksfiltrasi DNS dapat terjadi saat orang jahat menyusup ke instans aplikasi di VPC Anda dan kemudian menggunakan pencarian DNS untuk mengirim data keluar dari VPC ke domain yang mereka kontrol. Dengan DNS Firewall, Anda dapat memantau dan mengontrol domain yang dapat dimintai oleh aplikasi Anda. Anda dapat menolak akses ke domain yang Anda tahu buruk dan mengizinkan semua kueri lainnya untuk melewatinya. Sebagai alternatif, Anda dapat menolak akses ke semua domain kecuali domain yang Anda percayai secara eksplisit.

Anda juga dapat menggunakan DNS Firewall untuk memblokir permintaan resolusi ke sumber daya di zona yang di-hosting pribadi (bersama atau lokal) termasuk nama VPC endpoint. Itu juga dapat memblokir permintaan untuk nama EC2 instans Amazon publik atau pribadi.

DNS Firewall adalah fitur dari Route 53 VPC Resolver dan tidak memerlukan pengaturan VPC Resolver tambahan untuk digunakan.

AWS Firewall Manager mendukung DNS Firewall

Anda dapat menggunakan Firewall Manager untuk mengonfigurasi dan mengelola asosiasi grup aturan DNS Firewall secara terpusat untuk VPCs seluruh akun Anda. AWS Organizations Firewall Manager secara otomatis menambahkan asosiasi untuk VPCs itu masuk ke dalam cakupan kebijakan Firewall Manager DNS Firewall Anda. Untuk informasi selengkapnya, lihat [AWS Firewall Manager](#) di AWS WAF AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

Bagaimana DNS Firewall bekerja dengan AWS Network Firewall

DNS Firewall dan Network Firewall keduanya menawarkan penyaringan nama domain, tetapi untuk berbagai jenis lalu lintas. Dengan DNS Firewall dan Network Firewall bersama-sama, Anda dapat

mengonfigurasi pemfilteran berbasis domain untuk lalu lintas lapisan aplikasi melalui dua jalur jaringan yang berbeda.

- DNS Firewall menyediakan pemfilteran untuk kueri DNS keluar yang melewati Route 53 VPC Resolver dari aplikasi di dalam Anda. VPCs Anda juga dapat mengonfigurasi DNS Firewall untuk mengirim respons kustom untuk permintaan ke nama domain yang diblokir.
- Network Firewall menyediakan pemfilteran untuk lalu lintas lapisan jaringan dan aplikasi, tetapi tidak memiliki visibilitas ke dalam kueri yang dibuat oleh Route 53 VPC Resolver.

Untuk informasi selengkapnya tentang Network Firewall, lihat [Panduan Developer Network Firewall](#).

Cara kerja Resolver DNS Firewall

Resolver DNS Firewall memungkinkan Anda mengontrol akses ke situs dan memblokir ancaman tingkat DNS untuk kueri DNS yang keluar dari VPC Anda melalui Route 53 VPC Resolver. Dengan DNS Firewall, Anda menentukan aturan pemfilteran nama domain dalam grup aturan yang Anda kaitkan dengan Anda. VPCs Anda dapat menentukan daftar nama domain untuk mengizinkan atau memblokir, atau Resolver DNS Firewall Aturan lanjutan yang menawarkan perlindungan dari tunneling DNS dan ancaman berbasis Domain Generation Algorithm (DGA). Anda dapat menyesuaikan respons untuk kueri DNS yang Anda blokir. Untuk aturan yang berisi daftar domain, Anda juga dapat menyempurnakan aturan untuk mengizinkan jenis kueri tertentu, seperti MX-Records, melalui.

DNS Firewall hanya memfilter pada nama domain. Tidak menyelesaikan nama itu ke alamat IP yang akan diblokir. Selain itu, DNS Firewall menyaring lalu lintas DNS, tetapi tidak menyaring protokol lapisan aplikasi lainnya, seperti HTTPS, SSH, TLS, FTP, dan sebagainya.

Resolver DNS Firewall komponen dan pengaturan

Anda mengelola DNS Firewall dengan komponen pusat dan pengaturan berikut.

Kelompok aturan DNS Firewall

Mendefinisikan bernama, koleksi dapat digunakan kembali aturan DNS Firewall untuk menyaring permintaan DNS. Anda mengisi grup aturan dengan aturan pemfilteran, lalu mengaitkan grup aturan dengan satu atau lebih VPCs. Ketika Anda mengaitkan grup aturan dengan VPC, Anda mengaktifkan penyaringan DNS Firewall untuk VPC. Kemudian, ketika VPC Resolver menerima

kueri DNS untuk VPC yang memiliki grup aturan yang terkait dengannya, VPC Resolver meneruskan kueri ke DNS Firewall untuk difilter.

Jika Anda mengasosiasikan beberapa grup aturan dengan satu VPC, Anda menunjukkan urutan pemrosesannya melalui setelan prioritas di setiap asosiasi. DNS Firewall memproses grup aturan untuk VPC dari pengaturan prioritas numerik terendah ke atas.

Untuk informasi selengkapnya, lihat [Grup aturan dan aturan DNS Firewall](#).

Aturan DNS Firewall

Menentukan aturan pemfilteran untuk kueri DNS dalam grup aturan DNS Firewall. Setiap aturan menentukan satu daftar domain, atau perlindungan DNS Firewall dan tindakan untuk mengambil kueri DNS yang domainnya cocok dengan spesifikasi domain dalam aturan. Anda dapat mengizinkan (aturan hanya dengan daftar domain), memblokir, atau memperingatkan pada kueri yang cocok. Dalam aturan dengan daftar domain, Anda juga dapat menentukan jenis kueri untuk domain dalam daftar, misalnya, Anda dapat memblokir atau mengizinkan jenis kueri MX untuk domain atau domain tertentu. Anda juga dapat menentukan respon kustom untuk kueri yang diblokir.

Untuk aturan DNS Firewall, Anda hanya dapat memblokir atau memperingatkan pada kueri yang cocok.

Setiap aturan dalam grup aturan memiliki setelan prioritas yang unik dalam grup aturan. DNS Firewall memproses aturan dalam grup aturan dari pengaturan prioritas numerik terendah ke atas.

Aturan DNS Firewall hanya ada dalam konteks grup aturan tempat aturan tersebut ditetapkan. Anda tidak dapat menggunakan kembali aturan atau mereferensikannya terlepas dari grup aturannya.

Untuk informasi selengkapnya, lihat [Grup aturan dan aturan DNS Firewall](#).

Daftar domain

Mendefinisikan kumpulan spesifikasi domain bernama yang dapat digunakan kembali untuk digunakan dalam pemfilteran DNS. Setiap aturan dalam grup aturan memerlukan satu daftar domain. Anda dapat memilih untuk menentukan domain yang ingin Anda izinkan aksesnya, domain yang ingin Anda tolak aksesnya, atau kombinasi keduanya. Anda dapat membuat daftar domain Anda sendiri dan Anda dapat menggunakan daftar domain yang AWS mengelola untuk Anda.

Untuk informasi selengkapnya, lihat [Daftar domain DNS Firewall Resolver](#).

Pengaturan pengalihan domain (Hanya daftar Domain)

Pengaturan pengalihan domain memungkinkan Anda mengonfigurasi aturan DNS Firewall untuk memeriksa semua domain dalam rantai pengalihan DNS (default), seperti CNAME, DNAME, dll., Atau hanya domain pertama dan mempercayai sisanya. Jika Anda memilih untuk memeriksa seluruh rantai pengalihan DNS, Anda harus menambahkan domain berikutnya ke daftar domain yang disetel ke ALLOW dalam aturan. Jika Anda memilih untuk memeriksa seluruh rantai pengalihan DNS, Anda harus menambahkan domain berikutnya ke daftar domain dan mengatur tindakan yang ingin Anda ambil aturan, baik ALLOW, BLOCK, atau ALERT.

Untuk informasi selengkapnya, lihat [Pengaturan aturan di DNS Firewall](#).

Jenis kueri (hanya daftar Domain)

Pengaturan tipe kueri memungkinkan Anda mengonfigurasi aturan DNS Firewall untuk memfilter jenis kueri DNS tertentu. Jika Anda tidak memilih jenis kueri, aturan diterapkan ke semua jenis kueri DNS. Misalnya, Anda mungkin ingin memblokir semua jenis kueri untuk domain tertentu, tetapi mengizinkan catatan MX.

Untuk informasi selengkapnya, lihat [Pengaturan aturan di DNS Firewall](#).

DNS Firewall Perlindungan tingkat lanjut

Mendeteksi kueri DNS yang mencurigakan berdasarkan tanda tangan ancaman yang diketahui dalam kueri DNS. Setiap aturan dalam grup aturan memerlukan satu pengaturan perlindungan DNS Firewall Advanced. Anda dapat memilih perlindungan dari:

- Algoritma Pembuatan Domain () DGAs

DGAs digunakan oleh penyerang untuk menghasilkan sejumlah besar domain untuk meluncurkan serangan malware.

- Terowongan DNS

Tunneling DNS digunakan oleh penyerang untuk mengekstraksi data dari klien dengan menggunakan terowongan DNS tanpa membuat koneksi jaringan ke klien.

- Kamus DGA

Kamus DGAs digunakan oleh penyerang untuk menghasilkan domain menggunakan kata-kata kamus untuk menghindari deteksi dalam komunikasi malware. command-and-control

Dalam aturan DNS Firewall Advanced Anda dapat memilih untuk memblokir, atau memperingatkan pada kueri yang cocok dengan ancaman. Algoritma perlindungan ancaman dikelola dan diperbarui oleh AWS.

Untuk informasi selengkapnya, lihat [Resolver DNS Firewall Lanjutan](#).

Ambang kepercayaan (hanya perlindungan DNS Firewall Advanced)

Ambang batas kepercayaan untuk perlindungan ancaman DNS. Nilai ini harus diisi saat membuat aturan DNS Firewall Advanced. Nilai tingkat kepercayaan berarti:

- Tinggi – Hanya mendeteksi ancaman yang telah dikonfirmasi dengan tingkat false positive yang rendah.
- Sedang – Menyediakan keseimbangan antara deteksi ancaman dan false positive.
- Rendah – Memberikan tingkat deteksi tertinggi untuk ancaman, tetapi juga meningkatkan false positive.

Untuk informasi selengkapnya, lihat [Pengaturan aturan di DNS Firewall](#).

Asosiasi antara grup aturan DNS Firewall dan VPC

Mendefinisikan perlindungan untuk VPC menggunakan grup aturan DNS Firewall dan mengaktifkan konfigurasi VPC Resolver DNS Firewall untuk VPC.

Jika Anda mengasosiasikan beberapa grup aturan dengan satu VPC, Anda menunjukkan urutan pemrosesannya melalui setelan prioritas dalam asosiasi. DNS Firewall memproses grup aturan untuk VPC dari pengaturan prioritas numerik terendah ke atas.

Untuk informasi selengkapnya, lihat [Mengaktifkan perlindungan Resolver DNS Firewall untuk VPC Anda](#).

Konfigurasi DNS Firewall untuk VPC

Menentukan bagaimana VPC Resolver harus menangani perlindungan DNS Firewall di tingkat VPC. Konfigurasi ini berlaku setiap kali Anda memiliki setidaknya satu grup aturan DNS Firewall yang terkait dengan VPC.

Konfigurasi ini menentukan bagaimana Route 53 VPC Resolver menangani kueri ketika DNS Firewall gagal memfilternya. Secara default, jika VPC Resolver tidak menerima respons dari DNS Firewall untuk kueri, itu gagal ditutup dan memblokir kueri.

Untuk informasi selengkapnya, lihat [Konfigurasi VPC DNS Firewall](#).

Memantau tindakan DNS Firewall

Anda dapat menggunakan Amazon CloudWatch untuk memantau jumlah kueri DNS yang difilter oleh grup aturan DNS Firewall. CloudWatch mengumpulkan dan memproses data mentah menjadi metrik yang dapat dibaca, mendekati waktu nyata.

Untuk informasi selengkapnya, lihat [Memantau grup aturan DNS Firewall Resolver dengan Amazon CloudWatch](#).

Anda dapat menggunakan Amazon EventBridge, layanan tanpa server yang menggunakan peristiwa untuk menghubungkan komponen aplikasi bersama-sama, untuk membangun aplikasi berbasis peristiwa yang dapat diskalakan.

Untuk informasi selengkapnya, lihat [Mengelola peristiwa Resolver DNS Firewall menggunakan Amazon EventBridge](#).

Bagaimana Resolver DNS Firewall menyaring kueri DNS

Ketika grup aturan DNS Firewall dikaitkan dengan Resolver VPC Route 53 VPC VPC Anda, lalu lintas berikut difilter oleh firewall:

- Kueri DNS yang berasal dari VPC itu dan melewati VPC DNS.
- Permintaan DNS yang melewati titik akhir Resolver dari sumber daya lokal ke VPC yang sama yang memiliki DNS Firewall yang terkait dengan resolver.

Saat DNS Firewall menerima kueri DNS, DNS memfilter kueri menggunakan grup aturan, aturan, dan pengaturan lain yang telah Anda konfigurasi dan mengirimkan hasilnya kembali ke VPC Resolver:

- DNS Firewall mengevaluasi permintaan DNS menggunakan grup aturan yang terkait dengan VPC sampai menemukan kecocokan atau kehabisan semua kelompok aturan. DNS Firewall mengevaluasi kelompok aturan dalam urutan prioritas yang Anda tetapkan dalam asosiasi, dimulai dengan pengaturan numerik terendah. Untuk informasi selengkapnya, lihat [Grup aturan dan aturan DNS Firewall](#) dan [Mengaktifkan perlindungan Resolver DNS Firewall untuk VPC Anda](#).
- Dalam setiap grup aturan, DNS Firewall mengevaluasi kueri DNS terhadap daftar domain masing-masing aturan atau perlindungan DNS Firewall Advanced hingga menemukan kecocokan atau kehabisan semua aturan. DNS Firewall mengevaluasi aturan dalam urutan prioritas, dimulai dengan pengaturan numerik terendah. Untuk informasi selengkapnya, lihat [Grup aturan dan aturan DNS Firewall](#).

- Ketika DNS Firewall menemukan kecocokan dengan daftar domain aturan, atau anomali yang diidentifikasi oleh proteksi aturan DNS Firewall Advanced, itu mengakhiri evaluasi kueri dan merespons Resolver VPC dengan hasilnya. Jika tindakannya alert, DNS Firewall juga mengirimkan peringatan ke log Resolver VPC yang dikonfigurasi. Lihat informasi selengkapnya di [Aturan tindakan di DNS Firewall](#), [Daftar domain DNS Firewall Resolver](#), dan [Resolver DNS Firewall Lanjutan](#).
- Jika DNS Firewall mengevaluasi semua grup aturan tanpa menemukan kecocokan, DNS Firewall merespons kueri seperti biasa.

VPC Resolver merutekan kueri sesuai dengan respons dari DNS Firewall. Jika DNS Firewall gagal merespons, VPC Resolver menerapkan mode gagal DNS Firewall yang dikonfigurasi VPC. Untuk informasi selengkapnya, lihat [Konfigurasi VPC DNS Firewall](#).

Langkah-langkah tingkat tinggi untuk menggunakan Resolver DNS Firewall

Untuk menerapkan pemfilteran Resolver DNS Firewall di VPC Amazon Virtual Private Cloud, Anda melakukan langkah-langkah tingkat tinggi berikut.

- Tentukan pendekatan pemfilteran, daftar domain, atau perlindungan DNS Firewall — Tentukan cara memfilter kueri, mengidentifikasi spesifikasi domain yang Anda perlukan, dan tentukan logika yang akan Anda gunakan untuk mengevaluasi kueri. Misalnya, Anda mungkin ingin mengizinkan semua kueri kecuali kueri yang ada dalam daftar domain buruk yang diketahui. Atau Anda mungkin ingin melakukan yang sebaliknya dan memblokir semua kecuali daftar domain yang disetujui, dalam apa yang dikenal sebagai pendekatan walled garden. Anda dapat membuat dan mengelola daftar sendiri spesifikasi domain yang disetujui atau diblokir dan Anda dapat menggunakan daftar domain yang AWS mengelola untuk Anda. Untuk perlindungan DNS Firewall, Anda dapat memfilter kueri dengan memblokir semuanya, atau Anda dapat memberi tahu lalu lintas kueri yang mencurigakan ke domain yang mungkin berisi anomali yang terkait dengan ancaman (DGA, tunneling DNS, Dictionary DGA) untuk menguji pengaturan DNS Firewall Anda. Untuk informasi selengkapnya, lihat [Daftar domain DNS Firewall Resolver](#) dan [Resolver DNS Firewall Lanjutan](#).
- Membuat grup aturan firewall – Di DNS Firewall, buat grup aturan untuk memfilter kueri DNS untuk VPC Anda. Anda harus membuat grup aturan di setiap Wilayah tempat Anda ingin menggunakannya. Anda mungkin juga ingin memisahkan perilaku pemfilteran Anda menjadi lebih dari satu grup aturan untuk digunakan kembali dalam beberapa skenario pemfilteran untuk perbedaan Anda. VPCs Untuk informasi tentang grup aturan, lihat [Grup aturan dan aturan DNS Firewall](#).

- Menambahkan dan mengonfigurasi aturan Anda – Tambahkan aturan ke grup aturan Anda untuk setiap daftar domain dan perilaku pemfilteran yang Anda inginkan agar diberikan oleh grup aturan. Tetapkan setelan prioritas untuk aturan Anda sehingga aturan tersebut diproses dalam urutan yang benar dalam grup aturan, dengan memberikan prioritas terendah pada aturan yang ingin Anda evaluasi terlebih dahulu. Untuk informasi tentang aturan, lihat [Grup aturan dan aturan DNS Firewall](#).
- Kaitkan grup aturan ke VPC Anda – Untuk mulai menggunakan grup aturan DNS Firewall Anda, kaitkan dengan VPC Anda. Jika Anda menggunakan lebih dari satu grup aturan untuk VPC Anda, tetapkan prioritas setiap asosiasi sehingga grup aturan diproses dalam urutan yang benar, dengan memberikan prioritas terendah ke grup aturan yang ingin Anda evaluasi terlebih dahulu. Untuk informasi selengkapnya, lihat [Mengelola asosiasi antara grup aturan VPC dan Resolver DNS Firewall Anda](#).
- (Opsional) Ubah konfigurasi firewall untuk VPC — Jika Anda ingin Route 53 VPC Resolver memblokir kueri saat DNS Firewall gagal mengirim respons kembali untuk mereka, di VPC Resolver, ubah konfigurasi DNS Firewall VPC. Untuk informasi selengkapnya, lihat [Konfigurasi VPC DNS Firewall](#).

Menggunakan grup aturan Resolver DNS Firewall di beberapa Wilayah

Resolver DNS Firewall adalah layanan Regional, sehingga objek yang Anda buat di satu AWS Wilayah hanya tersedia di Wilayah tersebut. Untuk menggunakan grup aturan yang sama di lebih dari satu Wilayah, Anda harus membuatnya di setiap Wilayah.

AWS Akun yang membuat grup aturan dapat membagikannya dengan AWS akun lain. Untuk informasi selengkapnya, lihat [Berbagi grup aturan DNS Firewall Resolver antar akun AWS](#).

Ketersediaan wilayah untuk Resolver DNS Firewall

DNS Firewall tersedia sebagai berikut: Wilayah AWS

- Africa (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Malaysia)
- Asia Pacific (Melbourne)

- Asia Pasifik (Mumbai)
- Wilayah Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Thailand)
- Asia Pasifik (Tokyo)
- Wilayah Kanada (Pusat)
- Kanada Barat (Calgary)
- Wilayah Eropa (Frankfurt)
- Wilayah Eropa (Irlandia)
- Wilayah Eropa (London)
- Europe (Milan)
- Wilayah Eropa (Paris)
- Eropa (Spanyol)
- Eropa (Stockholm)
- Eropa (Zürich)
- Israel (Tel Aviv)
- Meksiko (Tengah)
- Timur Tengah (Bahrain)
- Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)
- AS Timur (Virginia Utara)
- AS Timur (Ohio)
- AS Barat (California Utara)
- AS Barat (Oregon)
- China (Beijing)
- China (Ningxia)
- AWS GovCloud (US)

Memulai dengan Resolver DNS Firewall

Konsol DNS Firewall menyertakan wizard yang memandu Anda melalui langkah-langkah berikut untuk memulai DNS Firewall:

- Buat grup aturan untuk setiap rangkaian aturan yang ingin Anda gunakan.
- Untuk setiap aturan, isi daftar domain yang ingin Anda periksa. Anda dapat membuat daftar domain Anda sendiri dan Anda dapat menggunakan daftar domain AWS terkelola.
- Kaitkan grup aturan Anda dengan VPCs tempat Anda ingin menggunakannya.

Contoh taman berdinding DNS Firewall Resolver

Dalam tutorial ini, Anda akan membuat grup aturan yang memblokir semua kecuali grup domain tertentu yang Anda percayai. Ini disebut platform tertutup, atau pendekatan walled garden.

Untuk mengonfigurasi grup aturan DNS Firewall menggunakan wizard konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon. Lanjutkan ke langkah 3.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka

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

2. Di panel navigasi, di bawah DNS Firewall, pilih Grup aturan.
3. Pada bilah navigasi, pilih Wilayah untuk grup aturan.
4. Di halaman Rule groups (Grup aturan), pilih Add rule group (Tambahkan grup aturan).
5. Untuk nama grup aturan, masukkan **WalledGardenExample**.

Di bagian Tag, Anda dapat secara opsional memasukkan pasangan kunci-nilai untuk tag. Tanda membantu Anda mengatur dan mengelola sumber daya AWS. Untuk informasi selengkapnya, lihat [Memberi tanda pada sumber daya Amazon Route 53](#).

6. Pilih Tambahkan grup aturan.

7. Pada halaman WalledGardenExampledetail, pilih tab Aturan, lalu Tambahkan aturan.
8. Di panel Rule Detail (Detail aturan), masukkan nama aturan **BlockAll**.
9. Di panel Domain list (Daftar domain), pilih Add my own domain list (Tambah daftar domain saya sendiri).
10. Di bagian Choose or create a new domain list (Pilih atau buat daftar domain baru), pilih Create new domain list (Buat daftar domain baru).
11. Masukkan nama daftar domain **AllDomains**, lalu di kotak teks Masukkan satu domain per baris, masukkan tanda bintang: *****.
12. Untuk pengaturan pengalihan Domain menerima default, dan biarkan jenis Query - opsional kosong.
13. Untuk Tindakan, pilih BLOCK dan kemudian biarkan respons untuk dikirim pada pengaturan default NODATA.
14. Pilih Tambahkan aturan. Aturan Anda BlockAllditampilkan di tab Aturan di WalledGardenExamplehalaman.
15. Pada WalledGardenExamplehalaman, pilih Tambahkan aturan untuk menambahkan aturan kedua ke grup aturan Anda.
16. Di panel Rincian aturan, masukkan nama **AllowSelectDomains** aturan.
17. Di panel Daftar domain, pilih Tambah daftar domain saya sendiri.
18. Di bagian Choose or create a new domain list (Pilih atau buat daftar domain baru), pilih Create new domain list (Buat daftar domain baru).
19. Masukkan nama daftar domain **ExampleDomains**.
20. Di kotak teks Masukkan satu domain per baris, pada baris pertama, masukkan **example.com** dan pada baris kedua, masukkan **example.org**.

 Note

Jika Anda ingin aturan berlaku juga untuk subdomain, Anda juga perlu menambahkan domain tersebut ke daftar. Misalnya, untuk menambahkan semua subdomain example.com, tambahkan ***.example.com** ke daftar.

21. Untuk pengaturan pengalihan Domain menerima default, dan biarkan jenis Query - opsional kosong.
22. Untuk Action, pilih ALLOW.

23. Pilih Add rule (Tambahkan aturan). Aturan Anda berdua ditampilkan di tab Aturan di WalledGardenExamplehalaman.
24. Di tab Aturan pada WalledGardenExamplehalaman, Anda dapat menyesuaikan urutan evaluasi aturan di grup aturan Anda dengan memilih nomor yang tercantum di kolom Prioritas dan mengetikkan nomor baru. DNS Firewall mengevaluasi aturan mulai dari pengaturan prioritas terendah, sehingga aturan dengan prioritas terendah adalah yang pertama dievaluasi. Untuk contoh ini, kami ingin DNS Firewall terlebih dahulu mengidentifikasi dan mengizinkan kueri DNS untuk daftar domain yang dipilih, lalu memblokir kueri yang tersisa.

Sesuaikan prioritas aturan sehingga AllowSelectDomainsmemiliki prioritas yang lebih rendah.

Anda sekarang memiliki grup aturan yang hanya mengizinkan kueri domain tertentu. Untuk mulai menggunakannya, Anda mengaitkannya dengan di VPCs mana Anda ingin menggunakan perilaku pemfilteran. Untuk informasi selengkapnya, lihat [Mengelola asosiasi antara grup aturan VPC dan Resolver DNS Firewall Anda](#).

Contoh daftar blok Resolver DNS Firewall

Dalam tutorial ini, Anda akan membuat grup aturan yang memblokir domain yang Anda tahu berbahaya. Anda juga akan menambahkan jenis kueri DNS yang diizinkan untuk domain dalam daftar yang diblokir. Grup aturan mengizinkan semua permintaan DNS keluar lainnya melalui Resolver VPC.

Untuk mengonfigurasi daftar blok DNS Firewall dengan menggunakan wizard konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon. Lanjutkan ke langkah 3.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>

2. Di panel navigasi, di bawah DNS Firewall, pilih Grup aturan.
3. Pada bilah navigasi, pilih Wilayah untuk grup aturan.
4. Di halaman Rule groups (Grup aturan), pilih Add rule group (Tambahkan grup aturan).

5. Untuk nama grup aturan, masukkan **BlockListExample**.

Di bagian Tag, Anda dapat secara opsional memasukkan pasangan kunci-nilai untuk tag. Tanda membantu Anda mengatur dan mengelola sumber daya AWS. Untuk informasi selengkapnya, lihat [Memberi tanda pada sumber daya Amazon Route 53](#).

6. Pada halaman BlockListExampleDetail, pilih tab Aturan, lalu Tambahkan aturan.
7. Di panel Rule Detail (Detail aturan), masukkan nama aturan **BlockList**.
8. Di panel Daftar domain, pilih Tambah daftar domain saya sendiri.
9. Di bagian Choose or create a new domain list (Pilih atau buat daftar domain baru), pilih Create new domain list (Buat daftar domain baru).
10. Masukkan nama daftar domain **MaliciousDomains**, lalu di kotak teks, masukkan domain yang ingin Anda blokir. Misalnya, **example.org**. Masukkan satu domain per baris.

 Note

Jika Anda ingin aturan berlaku juga untuk subdomain, Anda juga harus menambahkan domain tersebut ke daftar. Misalnya, untuk menambahkan semua subdomain example.org, tambahkan ***.example.org** ke daftar.

11. Untuk pengaturan pengalihan Domain menerima default, dan biarkan jenis Query - opsional kosong.
12. Untuk tindakan, pilih BLOCK dan biarkan respons untuk dikirim pada pengaturan default NODATA.
13. Pilih Add rule (Tambahkan aturan). Aturan Anda ditampilkan di tab Aturan di BlockListExampleDetail halaman.
14. di tab Aturan pada BlockedListExampleDetail halaman, Anda dapat menyesuaikan urutan evaluasi aturan di grup aturan Anda dengan memilih nomor yang tercantum di kolom Prioritas dan mengetikkan nomor baru. DNS Firewall mengevaluasi aturan mulai dari pengaturan prioritas terendah, sehingga aturan dengan prioritas terendah adalah yang pertama dievaluasi.

Pilih dan sesuaikan prioritas aturan sehingga BlockList dievaluasi baik sebelum atau sesudah aturan lain yang mungkin Anda miliki. Sebagian besar waktu, domain berbahaya yang diketahui harus diblokir terlebih dahulu. Artinya, aturan yang terkait dengannya harus memiliki nomor prioritas terendah.

15. Untuk menambahkan aturan yang memungkinkan data MX untuk BlockList domain, pada halaman BlockedListExampleDetail di tab Aturan, pilih Tambahkan aturan.

16. Di panel Rule Detail (Detail aturan), masukkan nama aturan **BlockList-allowMX**.
17. Di panel Domain list (Daftar domain), pilih Add my own domain list (Tambah daftar domain saya sendiri).
18. Di bawah Pilih atau buat daftar domain baru, pilih **MaliciousDomains**.
19. Untuk pengaturan pengalihan Domain, terima default.
20. Dalam daftar jenis kueri DNS, pilih MX: Menentukan server email.
21. Untuk tindakan, pilih ALLOW (IZINKAN).
22. Pilih Add rule (Tambahkan aturan).
23. di tab Aturan pada BlockedListExamplehalaman, Anda dapat menyesuaikan urutan evaluasi aturan di grup aturan Anda dengan memilih nomor yang tercantum di kolom Prioritas dan mengetikkan nomor baru. DNS Firewall mengevaluasi aturan mulai dari pengaturan prioritas terendah, sehingga aturan dengan prioritas terendah adalah yang pertama dievaluasi.

Pilih dan sesuaikan prioritas aturan sehingga BlockList-AllowMX dievaluasi baik sebelum atau sesudah aturan lain yang mungkin Anda miliki. Karena Anda ingin mengizinkan kueri MX, pastikan bahwa aturan BlockList-AllowMX memiliki prioritas yang lebih rendah daripada BlockList

Anda sekarang memiliki grup aturan yang memblokir kueri domain berbahaya tertentu, tetapi memungkinkan jenis kueri DNS tertentu. Untuk mulai menggunakannya, Anda mengaitkannya dengan di VPCs mana Anda ingin menggunakan perilaku pemfilteran. Untuk informasi selengkapnya, lihat [Mengelola asosiasi antara grup aturan VPC dan Resolver DNS Firewall Anda](#).

Grup aturan dan aturan DNS Firewall

Bagian ini menjelaskan pengaturan yang dapat Anda konfigurasikan untuk grup dan aturan aturan DNS Firewall Anda, untuk menentukan perilaku DNS Firewall untuk Anda. VPCs Ini juga menjelaskan cara mengelola pengaturan untuk grup dan aturan aturan Anda.

Saat Anda memiliki grup aturan yang dikonfigurasi seperti yang Anda inginkan, Anda menggunakannya secara langsung dan Anda dapat berbagi serta mengelolanya antar akun dan di seluruh organisasi Anda di AWS Organizations.

- Anda dapat mengaitkan grup aturan dengan beberapa VPCs, untuk memberikan perilaku yang konsisten di seluruh organisasi Anda. Untuk informasi, lihat [Mengelola asosiasi antara grup aturan VPC dan Resolver DNS Firewall Anda](#).

- Anda dapat berbagi grup aturan di antara akun, untuk manajemen kueri DNS yang konsisten di seluruh organisasi Anda. Untuk informasi, lihat [Berbagi grup aturan DNS Firewall Resolver antar akun AWS](#).
- Anda dapat menggunakan grup aturan di seluruh organisasi Anda AWS Organizations dengan mengelolanya dalam AWS Firewall Manager kebijakan. Untuk informasi tentang Firewall Manager, lihat [AWS Firewall Manager](#) di AWS WAF, AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

Pengaturan grup aturan di DNS Firewall

Saat Anda membuat atau mengedit grup aturan DNS Firewall, Anda menentukan nilai berikut:

Nama

Nama unik yang memudahkan Anda menemukan grup aturan di dasbor.

Deskripsi (Opsional)

Deskripsi singkat yang memberikan lebih banyak konteks untuk grup aturan.

Region

AWS Wilayah yang Anda pilih saat Anda membuat grup aturan. Grup aturan yang Anda buat di satu Wilayah hanya tersedia di Wilayah itu. Untuk menggunakan grup aturan yang sama di lebih dari satu Wilayah, Anda harus membuatnya di setiap Wilayah.

Aturan

Perilaku pemfilteran grup aturan terkandung dalam aturannya. Untuk informasi, lihat bagian berikut.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Ini adalah tag yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Gunakan Tanda Alokasi Biaya](#) dalam Panduan Pengguna AWS Billing .

Pengaturan aturan di DNS Firewall

Saat Anda membuat atau mengedit aturan di grup aturan DNS Firewall, Anda menentukan nilai berikut:

Nama

Pengidentifikasi unik untuk aturan dalam grup aturan.

Deskripsi (Opsional)

Deskripsi singkat yang memberikan informasi lebih lanjut tentang aturan.

Daftar domain

Daftar domain yang diperiksa oleh aturan. Anda dapat membuat dan mengelola daftar domain Anda sendiri atau Anda dapat berlangganan daftar domain yang dikelola AWS untuk Anda. Untuk informasi selengkapnya, lihat [Daftar domain DNS Firewall Resolver](#).

Aturan dapat berisi eter daftar domain atau perlindungan DNS Firewall Advanced, tetapi tidak keduanya.

Pengaturan pengalihan domain (hanya daftar domain)

Anda dapat memilih aturan DNS Firewall untuk memeriksa hanya domain pertama atau semua (default) domain dalam rantai pengalihan DNS, seperti CNAME, DNAME, dll. Jika Anda memilih untuk memeriksa semua domain, Anda harus menambahkan domain berikutnya dalam rantai pengalihan DNS ke daftar domain dan mengatur ke tindakan yang Anda ingin aturan untuk mengambil, baik ALLOW, BLOCK, atau ALERT. Untuk informasi selengkapnya, lihat [Resolver DNS Firewall komponen dan pengaturan](#).

Jenis kueri (hanya daftar domain)

Daftar jenis kueri DNS yang diperiksa aturan. Berikut ini adalah nilai yang valid:

- A: Mengembalikan IPv4 alamat.
- AAAA: Mengembalikan alamat Ipv6.
- CAA: Membatasi CAs yang dapat membuat SSL/TLS sertifikasi untuk domain.
- CNAME: Mengembalikan nama domain lain.
- DS: Rekam yang mengidentifikasi kunci penandatanganan DNSSEC dari zona yang didelegasikan.
- MX: Menentukan server email.
- NAPTR: Regular-expression-based menulis ulang nama domain.

- NS: Server nama otoritatif.
- PTR: Memetakan alamat IP ke nama domain.
- SOA: Mulai dari catatan otoritas untuk zona tersebut.
- SPF: Daftar server yang berwenang untuk mengirim email dari domain.
- SRV: Nilai spesifik aplikasi yang mengidentifikasi server.
- TXT: Memverifikasi pengirim email dan nilai khusus aplikasi.
- Jenis kueri yang Anda tentukan dengan menggunakan ID tipe DNS, misalnya 28 untuk AAAA. Nilai harus didefinisikan sebagai TYPE **NUMBER**, di mana **NUMBER** bisa 1-65534, misalnya, TYPE28 Untuk informasi selengkapnya, lihat [Daftar jenis rekaman DNS](#).

Anda dapat membuat satu jenis kueri per aturan.

 Note

Jika Anda mengatur aturan BLOCK firewall dengan tindakan NXDOMAIN pada jenis kueri sama dengan AAAA, tindakan ini tidak akan diterapkan ke IPv6 alamat sintetis yang dihasilkan saat diaktifkan. DNS64

DNS Firewall Perlindungan tingkat lanjut

Mendeteksi kueri DNS yang mencurigakan berdasarkan tanda tangan ancaman yang diketahui dalam kueri DNS. Anda dapat memilih perlindungan dari:

- Algoritma Pembuatan Domain () DGAs

DGAs digunakan oleh penyerang untuk menghasilkan sejumlah besar domain untuk meluncurkan serangan malware.

- Terowongan DNS

Tunneling DNS digunakan oleh penyerang untuk mengekstraksi data dari klien dengan menggunakan terowongan DNS tanpa membuat koneksi jaringan ke klien.

- Kamus DGA

Kamus DGAs digunakan oleh penyerang untuk menghasilkan domain menggunakan kata-kata kamus untuk menghindari deteksi dalam komunikasi malware. command-and-control

Dalam aturan DNS Firewall Advanced Anda dapat memilih untuk memblokir, atau memperingatkan pada kueri yang cocok dengan ancaman.

Untuk informasi lebih lanjut, lihat [Untuk informasi lebih lanjut, lihat Resolver DNS Firewall Lanjutan](#).

Aturan dapat berisi eter perlindungan DNS Firewall Advanced atau daftar domain, tetapi tidak keduanya.

Ambang kepercayaan (DNS Firewall Advanced saja)

Ambang batas kepercayaan untuk DNS Firewall Advanced. Nilai ini harus diisi saat membuat aturan DNS Firewall Advanced. Nilai tingkat kepercayaan berarti:

- Tinggi – Hanya mendeteksi ancaman yang telah dikonfirmasi dengan tingkat false positive yang rendah.
- Sedang – Menyediakan keseimbangan antara deteksi ancaman dan false positive.
- Rendah – Memberikan tingkat deteksi tertinggi untuk ancaman, tetapi juga meningkatkan false positive.

Untuk informasi selengkapnya, lihat [Pengaturan aturan di DNS Firewall](#).

Tindakan

Bagaimana Anda ingin DNS Firewall menangani kueri DNS yang nama domainnya cocok dengan spesifikasi dalam daftar domain aturan. Untuk informasi selengkapnya, lihat [Aturan tindakan di DNS Firewall](#).

Prioritas

Setelan bilangan bulat positif unik untuk aturan dalam grup aturan yang menentukan urutan pemrosesan. DNS Firewall memeriksa kueri DNS terhadap aturan dalam grup aturan dimulai dengan pengaturan prioritas numerik terendah dan naik. Anda dapat mengubah prioritas aturan kapan saja, misalnya mengubah urutan pemrosesan atau memberi ruang untuk aturan lain.

Aturan tindakan di DNS Firewall

Saat DNS Firewall menemukan kecocokan antara kueri DNS dan spesifikasi domain dalam aturan, hal ini menerapkan tindakan yang ditentukan dalam aturan ke kueri.

Anda harus menentukan salah satu opsi berikut di setiap aturan yang Anda buat:

- Allow— Berhenti memeriksa kueri dan membiarkannya masuk. Tidak tersedia untuk DNS Firewall Advanced.

- **Alert**— Berhenti memeriksa kueri, izinkan untuk melewati, dan catat peringatan untuk kueri di log Resolver VPC Route 53.
- **Block**— Hentikan pemeriksaan kueri, blokir agar tidak pergi ke tujuan yang dimaksudkan, dan catat tindakan blok untuk kueri di log Resolver VPC Route 53.

Balas dengan respons blok yang dikonfigurasi, dari berikut ini:

- **NODATA**— Menanggapi yang menunjukkan bahwa kueri berhasil, tetapi tidak ada respons yang tersedia untuk itu.
- **NXDOMAIN**— Menanggapi yang menunjukkan bahwa nama domain kueri tidak ada.
- **OVERRIDE**— Berikan penggantian khusus dalam respons. Opsi ini memerlukan pengaturan tambahan sebagai berikut:
 - **Record value**— Catatan DNS khusus untuk dikirim kembali sebagai respons terhadap kueri.
 - **Record type**— Jenis catatan DNS. Ini akan menentukan format nilai catatan. Ini harus CNAME.
 - **Time to live in seconds**— Jumlah waktu yang disarankan untuk resolver DNS atau browser web untuk menyimpan catatan override dan menggunakannya sebagai respons terhadap kueri ini, jika diterima lagi. Secara default, ini adalah nol, dan catatan tidak di-cache.

Untuk informasi selengkapnya tentang konfigurasi log kueri dan konten, lihat [Pencatatan kueri penyelesai](#) dan [Nilai yang muncul di log kueri VPC Resolver](#).

Gunakan Alert untuk menguji aturan pemblokiran

Saat pertama kali membuat aturan pemblokiran, Anda dapat mengujinya dengan mengonfigurasinya dengan tindakan yang disetel ke Alert. Anda kemudian dapat melihat jumlah kueri yang diperingatkan aturan untuk melihat berapa banyak yang akan diblokir jika Anda menyetel tindakan ke Block.

Mengelola grup aturan dan aturan di DNS Firewall

Untuk mengelola grup aturan dan aturan di konsol, ikuti panduan di bagian ini.

Saat Anda membuat perubahan pada entitas DNS Firewall, seperti aturan dan daftar domain, DNS Firewall menyebarkan perubahan di mana pun entitas tersebut disimpan dan digunakan. Perubahan Anda diterapkan dalam hitungan detik, tetapi mungkin ada periode inkonsistensi singkat saat perubahan telah tiba di beberapa tempat dan tidak di tempat lain. Jadi, misalnya, jika Anda menambahkan domain ke daftar domain yang direferensikan oleh aturan pemblokiran, domain baru mungkin diblokir sebentar di satu area VPC Anda sementara masih diizinkan di area lain. Inkonsistensi sementara ini dapat terjadi saat Anda pertama kali mengonfigurasi asosiasi grup aturan

dan VPC, serta saat Anda mengubah setelan yang ada. Umumnya, inkonsistensi jenis ini hanya bertahan beberapa detik.

Membuat grup aturan dan aturan

Untuk membuat grup aturan dan menambahkan aturan ke dalamnya, ikuti langkah-langkah dalam prosedur ini.

Untuk membuat grup aturan dan aturannya

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon. Lanjutkan ke langkah 3.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka

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

2. Di panel navigasi, di bawah DNS Firewall, pilih Grup aturan.
3. Pada bilah navigasi, pilih Wilayah untuk grup aturan.
4. Pilih Add rule group (Tambahkan grup aturan), lalu ikuti panduan wizard untuk menentukan grup aturan dan pengaturan aturan Anda.

Untuk informasi tentang nilai untuk grup aturan, lihat [Pengaturan grup aturan di DNS Firewall](#).

Untuk informasi tentang nilai aturan, lihat [Pengaturan aturan di DNS Firewall](#).

Melihat dan memperbarui grup aturan dan aturan

Gunakan prosedur berikut untuk melihat grup aturan dan aturan yang ditetapkan untuk mereka. Anda juga dapat memperbarui grup aturan dan pengaturan aturan.

Untuk melihat dan memperbarui grup aturan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon. Lanjutkan ke langkah 3.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka

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

2. Di panel navigasi, di bawah DNS Firewall, pilih Grup aturan.
3. Pada bilah navigasi, pilih Wilayah untuk grup aturan.
4. Pilih grup aturan yang ingin Anda lihat atau edit, lalu pilih Lihat detail.
5. Di halaman grup aturan, Anda dapat melihat dan mengedit pengaturan.

Untuk informasi tentang nilai untuk grup aturan, lihat [Pengaturan grup aturan di DNS Firewall](#).

Untuk informasi tentang nilai aturan, lihat [Pengaturan aturan di DNS Firewall](#).

Menghapus grup aturan

Untuk menghapus grup aturan, lakukan prosedur berikut.

Important

Jika Anda menghapus grup aturan yang terkait dengan VPC, DNS Firewall akan menghapus asosiasi dan menghentikan perlindungan yang diberikan grup aturan ke VPC.

Menghapus entitas DNS Firewall

Saat Anda menghapus entitas yang dapat Anda gunakan di DNS Firewall, seperti daftar domain yang mungkin digunakan dalam grup aturan, atau grup aturan yang mungkin terkait dengan VPC, DNS Firewall akan memeriksa untuk melihat apakah entitas saat ini sedang digunakan. Jika entitas sedang digunakan, DNS Firewall akan memperingatkan Anda. DNS Firewall hampir selalu dapat menentukan apakah entitas sedang digunakan. Namun, dalam kasus yang jarang terjadi mungkin DNS Firewall tidak dapat melakukannya. Jika Anda perlu memastikan bahwa saat ini tidak ada yang menggunakan entitas, periksa di konfigurasi DNS Firewall Anda sebelum menghapusnya. Jika entitas adalah daftar domain yang direferensikan, periksa apakah tidak ada grup aturan yang

menggunakannya. Jika entitas adalah grup aturan, periksa apakah entitas tersebut tidak terkait dengan apa pun VPCs.

Untuk menghapus grup aturan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon. Lanjutkan ke langkah 3.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka

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

2. Di panel navigasi, di bawah DNS Firewall, pilih Grup aturan.
3. Pada bilah navigasi, pilih Wilayah untuk grup aturan.
4. Pilih grup aturan yang ingin Anda hapus, lalu pilih Hapus, dan konfirmasi penghapusan.

Daftar domain DNS Firewall Resolver

Daftar domain adalah seperangkat spesifikasi domain yang dapat digunakan kembali yang Anda gunakan dalam aturan DNS Firewall, di dalam grup aturan. Ketika Anda mengasosiasikan grup aturan dengan VPC, DNS Firewall membandingkan kueri DNS Anda terhadap daftar domain yang digunakan dalam aturan. Jika menemukan kecocokan, DNS Firewall akan menangani kueri DNS sesuai dengan tindakan aturan pencocokan ini. Untuk informasi selengkapnya tentang grup aturan dan aturan, lihat [Grup aturan dan aturan DNS Firewall](#).

Daftar domain memungkinkan Anda untuk memisahkan spesifikasi domain eksplisit dari tindakan yang ingin Anda lakukan. Anda dapat menggunakan satu daftar domain dalam beberapa aturan dan pembaruan apa pun yang Anda lakukan pada daftar domain secara otomatis memengaruhi semua aturan yang menggunakannya.

Daftar domain dibagi dalam dua kategori utama:

- Daftar domain terkelola, yang AWS membuat dan memelihara untuk Anda.
- Daftar domain Anda sendiri, yang Anda buat dan kelola.

Bagian ini menjelaskan jenis daftar domain terkelola yang tersedia untuk Anda dan memberikan panduan untuk membuat dan mengelola daftar domain Anda sendiri, jika Anda memilih untuk melakukannya.

Daftar Domain Terkelola

Daftar Domain Terkelola berisi nama domain yang terkait dengan aktivitas berbahaya atau potensi ancaman lainnya. AWS memelihara daftar ini untuk memungkinkan pelanggan Route 53 VPC Resolver untuk memeriksa kueri DNS keluar terhadap mereka secara gratis saat menggunakan DNS Firewall.

Terus memantau kondisi terbaru terkait lanskap ancaman yang terus berubah dapat memakan waktu dan biaya yang besar. Daftar Domain Terkelola dapat menghemat waktu Anda saat menerapkan dan menggunakan DNS Firewall. AWS secara otomatis memperbarui daftar ketika kerentanan dan ancaman baru muncul. AWS sering diberitahu tentang kerentanan baru sebelum pengungkapan publik, sehingga DNS Firewall dapat menyebarkan mitigasi untuk Anda sering sebelum ancaman baru telah dikenal luas.

Daftar domain terkelola dirancang untuk membantu melindungi Anda dari ancaman web umum dan menambahkan lapisan keamanan lain untuk aplikasi Anda. Daftar Domain AWS Terkelola sumber data mereka dari kedua AWS sumber internal maupun [RecordedFuture](#), dan terus diperbarui. Namun, Daftar Domain AWS Terkelola tidak dimaksudkan sebagai pengganti kontrol keamanan lainnya, seperti Amazon GuardDuty, yang ditentukan oleh AWS sumber daya yang Anda pilih.

Sebagai praktik terbaik, sebelum menggunakan Daftar Domain Terkelola dalam produksi, ujilah di lingkungan non-produksi, dengan tindakan aturan disetel keAlert. Evaluasi aturan menggunakan CloudWatch metrik Amazon yang dikombinasikan dengan permintaan sampel Resolver DNS Firewall atau log DNS Firewall. Saat Anda puas bahwa aturan melakukan apa yang Anda inginkan, ubah setelan tindakan sesuai kebutuhan.

Daftar Domain AWS Terkelola yang Tersedia

Bagian ini menjelaskan Daftar Domain Terkelola yang saat ini tersedia. Saat berada di Wilayah tempat daftar ini didukung, Anda melihatnya di konsol saat mengelola daftar domain dan saat menentukan daftar domain untuk aturan. Dalam log, daftar domain dicatat dalam `firewall_domain_list_id` field.

AWS menyediakan Daftar Domain Terkelola berikut, di Wilayah yang tersedia, untuk semua pengguna Resolver DNS Firewall.

- **AWSManagedDomainsMalwareDomainList** – Domain yang terkait dengan pengiriman malware, meng-host malware, atau mendistribusikan malware.
- **AWSManagedDomainsBotnetCommandandControl**– Domain yang terkait dengan pengendalian jaringan komputer yang terinfeksi malware spamming.
- **AWSManagedDomainsAggregateThreatList**— Domain yang terkait dengan beberapa kategori ancaman DNS termasuk malware, ransomware, botnet, spyware, dan tunneling DNS untuk membantu memblokir berbagai jenis ancaman. **AWSManagedDomainsAggregateThreatList**mencakup semua domain dalam Daftar Domain AWS Terkelola lainnya yang tercantum di sini.
- **AWSManagedDomainsAmazonGuardDutyThreatList**— Domain yang terkait dengan temuan keamanan GuardDuty DNS Amazon. Domain bersumber dari sistem intelijen ancaman GuardDuty saja, dan tidak mengandung domain yang bersumber dari sumber pihak ketiga eksternal. Lebih khusus lagi, saat ini daftar ini hanya akan memblokir domain yang dibuat secara internal dan digunakan untuk deteksi berikut di GuardDuty: `Impact:/.Reputation`, `Impact:EC2/AbusedDomainRequest.Reputation`, `Impact:EC2/BitcoinDomainRequest.Reputation`, `Impact:EC2 .ReputationMaliciousDomainRequest`, `Runtime/AbusedDomainRequest.Reputation`, `Impact:Runtime/BitcoinDomainRequest.Reputation`, and `Impact:Runtime/MaliciousDomainRequest`

Untuk informasi selengkapnya, lihat [Menemukan jenis](#) di Panduan GuardDuty Pengguna Amazon.

AWS Daftar Domain Terkelola tidak dapat diunduh atau dijelajahi. Untuk melindungi kekayaan intelektual, Anda tidak dapat melihat atau mengedit spesifikasi domain individual dalam Daftar Domain AWS Terkelola. Pembatasan ini juga membantu mencegah pengguna jahat merancang ancaman yang secara khusus menghindari daftar yang dipublikasikan.

Untuk menguji daftar Domain Terkelola

Kami menyediakan kumpulan domain berikut untuk menguji Daftar Domain Terkelola:

AWSManagedDomainsBotnetCommandandControl

- `controldomain1.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain2.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain3.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com`

AWSManagedDomainsMalwareDomainList

- `controldomain1.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain2.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com`

- `controldomain3.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com`

`AWSManagedDomainsAggregateThreatList` dan `AWSManagedDomainsAmazonGuardDutyThreatList`

- `controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com`
- `controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com`

Domain ini akan diselesaikan ke 1.2.3.4 jika tidak diblokir. Jika Anda menggunakan Daftar Domain Terkelola di VPC, kueri untuk domain ini akan menampilkan respons yang disetel ke tindakan pemblokiran dalam aturan (misalnya NODATA).

Untuk informasi selengkapnya tentang Daftar Domain Terkelola, hubungi [AWS Dukungan Pusat](#).

Tabel berikut mencantumkan ketersediaan Wilayah untuk Daftar Domain AWS Terkelola.

Daftar Domain Terkelola Ketersediaan wilayah

Region	Daftar Domain Terkelola tersedia?
Africa (Cape Town)	Ya
Asia Pasifik (Hong Kong)	Ya
Asia Pasifik (Hyderabad)	Ya
Asia Pasifik (Jakarta)	Ya
Asia Pasifik (Malaysia)	Ya
Asia Pacific (Melbourne)	Ya
Asia Pasifik (Mumbai)	Ya
Wilayah Asia Pasifik (Osaka)	Ya

Region	Daftar Domain Terkelola tersedia?
Asia Pasifik (Seoul)	Ya
Asia Pacific (Singapore)	Ya
Asia Pasifik (Sydney)	Ya
Asia Pasifik (Thailand)	Ya
Asia Pasifik (Tokyo)	Ya
Wilayah Kanada (Pusat)	Ya
Kanada Barat (Calgary)	Ya
Wilayah Eropa (Frankfurt)	Ya
Wilayah Eropa (Irlandia)	Ya
Wilayah Eropa (London)	Ya
Europe (Milan)	Ya
Wilayah Eropa (Paris)	Ya
Eropa (Spanyol)	Ya
Eropa (Stockholm)	Ya

Region	Daftar Domain Terkelola tersedia?
Europe (Zurich)	Ya
Israel (Tel Aviv)	Ya
Timur Tengah (Bahrain)	Ya
Timur Tengah (UAE)	Ya
Amerika Selatan (Sao Paulo)	Ya
AS Timur (Virginia Utara)	Ya
AS Timur (Ohio)	Ya
AS Barat (California Utara)	Ya
AS Barat (Oregon)	Ya
Tiongkok (Beijing)	Ya
Tiongkok (Ningxia)	Ya
AWS GovCloud (US)	Ya

Pertimbangan keamanan tambahan

AWS Daftar Domain Terkelola dirancang untuk membantu melindungi Anda dari ancaman web umum. Ketika digunakan sesuai dengan dokumentasi, daftar ini menambahkan lapisan keamanan lain untuk aplikasi Anda. Namun, Daftar Domain Terkelola tidak dimaksudkan sebagai pengganti kontrol keamanan lainnya, yang ditentukan oleh AWS sumber daya yang Anda pilih. Untuk

memastikan bahwa sumber daya Anda AWS dilindungi dengan benar, lihat panduan di [Model Tanggung Jawab Bersama](#).

Mengurangi skenario positif palsu

Jika Anda menghadapi skenario positif palsu dalam aturan yang menggunakan Daftar Domain Terkelola untuk memblokir kueri, lakukan langkah-langkah berikut:

1. Dalam log Resolver VPC, identifikasi grup aturan dan daftar domain terkelola yang menyebabkan positif palsu. Anda melakukan ini dengan menemukan log untuk kueri yang diblokir oleh DNS Firewall, tetapi yang ingin Anda izinkan. Catatan log mencantumkan grup aturan, tindakan aturan, dan daftar terkelola. Untuk informasi lebih lanjut tentang log, lihat [Nilai yang muncul di log kueri VPC Resolver](#).
2. Buat aturan baru di grup aturan yang secara eksplisit mengizinkan kueri yang diblokir. Saat Anda membuat aturan, Anda dapat menentukan daftar domain Anda sendiri hanya dengan spesifikasi domain yang ingin Anda izinkan. Ikuti panduan untuk grup aturan dan manajemen aturan di [Membuat grup aturan dan aturan](#).
3. Prioritaskan aturan baru di dalam grup aturan sehingga berjalan sebelum aturan yang menggunakan daftar terkelola. Untuk melakukan ini, berikan aturan baru pengaturan prioritas numerik yang lebih rendah.

Saat Anda telah memperbarui grup aturan, aturan baru akan secara eksplisit mengizinkan nama domain yang ingin Anda izinkan sebelum aturan pemblokiran berjalan.

Mengelola daftar domain Anda sendiri

Anda dapat membuat daftar domain Anda sendiri untuk menentukan kategori domain yang tidak Anda temukan di penawaran daftar domain terkelola atau yang Anda pilih untuk tangani sendiri.

Selain prosedur yang dijelaskan di bagian ini, di konsol, Anda dapat membuat daftar domain dalam konteks manajemen aturan Resolver DNS Firewall, saat Anda membuat atau memperbarui aturan.

Setiap spesifikasi domain dalam daftar domain Anda harus memenuhi persyaratan berikut:

- Secara opsional dapat diawali dengan * (tanda bintang).
- Dengan pengecualian tanda bintang awal opsional dan titik, sebagai pembatas antara label, itu hanya boleh berisi karakter berikut: A-Z, a-z 0-9, - (tanda hubung).
- Panjangnya harus antara 1-255 karakter.

Saat Anda membuat perubahan pada entitas DNS Firewall, seperti aturan dan daftar domain, DNS Firewall menyebarkan perubahan di mana pun entitas tersebut disimpan dan digunakan. Perubahan Anda diterapkan dalam hitungan detik, tetapi mungkin ada periode inkonsistensi singkat saat perubahan telah tiba di beberapa tempat dan tidak di tempat lain. Jadi, misalnya, jika Anda menambahkan domain ke daftar domain yang direferensikan oleh aturan pemblokiran, domain baru mungkin diblokir sebentar di satu area VPC Anda sementara masih diizinkan di area lain. Inkonsistensi sementara ini dapat terjadi saat Anda pertama kali mengonfigurasi asosiasi grup aturan dan VPC, serta saat Anda mengubah setelan yang ada. Umumnya, inkonsistensi jenis ini hanya bertahan beberapa detik.

Uji daftar domain Anda sebelum menggunakannya dalam produksi

Sebagai praktik terbaik, sebelum menggunakan daftar domain dalam produksi, uji di lingkungan nonproduksi, dengan tindakan aturan diatur ke `Alert`. Evaluasi aturan menggunakan CloudWatch metrik Amazon dan log Resolver VPC. Log memberikan nama daftar domain untuk semua peringatan dan tindakan pemblokiran. Saat Anda puas bahwa daftar domain cocok dengan kueri DNS seperti yang Anda inginkan, ubah setelan tindakan aturan sesuai kebutuhan. Untuk informasi tentang CloudWatch metrik dan log kueri, lihat [Memantau grup aturan DNS Firewall Resolver dengan Amazon CloudWatch](#), [Nilai yang muncul di log kueri VPC Resolver](#), dan [Mengelola konfigurasi pencatatan kueri Resolver](#).

Untuk menambahkan daftar domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon. Lanjutkan ke langkah 2.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka

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

2. Di panel navigasi, di bawah DNS Firewall, pilih Daftar domain. Di halaman Domain lists (Daftar domain), Anda dapat memilih dan mengedit daftar domain yang ada dan Anda dapat menambahkan sendiri.
3. Untuk menambahkan daftar domain, pilih Add domain list (Tambah daftar domain).

4. Berikan nama untuk daftar domain Anda, dan kemudian masukkan spesifikasi domain Anda dalam kotak teks, satu per baris.

Jika Anda menggeser Switch to bulk upload (Alihkan ke unggahan massal) ke on (aktif), masukkan URI bucket Amazon S3 tempat Anda membuat daftar domain. Daftar domain ini harus memiliki satu nama domain per baris.

 Note

Nama domain duplikat akan menyebabkan impor massal gagal.

5. Pilih Add domain list (Tambah daftar domain). Halaman Domain lists (Daftar domain) mencantumkan daftar domain baru Anda.

Setelah Anda membuat daftar domain, Anda dapat merujuknya dengan nama dari aturan DNS Firewall Anda.

Menghapus entitas DNS Firewall

Saat Anda menghapus entitas yang dapat Anda gunakan di DNS Firewall, seperti daftar domain yang mungkin digunakan dalam grup aturan, atau grup aturan yang mungkin terkait dengan VPC, DNS Firewall akan memeriksa untuk melihat apakah entitas saat ini sedang digunakan. Jika entitas sedang digunakan, DNS Firewall akan memperingatkan Anda. DNS Firewall hampir selalu dapat menentukan apakah entitas sedang digunakan. Namun, dalam kasus yang jarang terjadi mungkin DNS Firewall tidak dapat melakukannya. Jika Anda perlu memastikan bahwa saat ini tidak ada yang menggunakan entitas, periksa di konfigurasi DNS Firewall Anda sebelum menghapusnya. Jika entitas adalah daftar domain yang direferensikan, periksa apakah tidak ada grup aturan yang menggunakannya. Jika entitas adalah grup aturan, periksa apakah entitas tersebut tidak terkait dengan apa pun VPCs.

Cara menghapus daftar domain

1. Di panel navigasi, pilih Domain lists (Daftar domain).
2. Pada bilah navigasi, pilih Wilayah untuk daftar domain.
3. Pilih daftar domain yang ingin Anda hapus, lalu pilih Hapus, dan konfirmasi penghapusan.

Resolver DNS Firewall Lanjutan

DNS Firewall Advanced mendeteksi kueri DNS yang mencurigakan berdasarkan tanda tangan ancaman yang diketahui dalam kueri DNS. Anda dapat menentukan jenis ancaman dalam aturan yang Anda gunakan dalam aturan DNS Firewall, di dalam grup aturan. Saat Anda mengaitkan grup aturan dengan VPC, DNS Firewall membandingkan kueri DNS Anda dengan domain yang ditandai dalam aturan. Jika menemukan kecocokan, DNS Firewall akan menangani kueri DNS sesuai dengan tindakan aturan pencocokan ini.

DNS Firewall Advanced bekerja dengan mengidentifikasi tanda tangan ancaman DNS yang mencurigakan dengan memeriksa berbagai pengidentifikasi kunci dalam muatan DNS termasuk stempel waktu permintaan, frekuensi permintaan dan tanggapan, string kueri DNS, dan panjang, jenis atau ukuran kueri DNS keluar dan masuk. Berdasarkan jenis tanda tangan ancaman, Anda dapat mengonfigurasi kebijakan untuk memblokir, atau cukup log dan peringatan pada kueri. Dengan menggunakan serangkaian pengidentifikasi ancaman yang diperluas, Anda dapat melindungi terhadap ancaman DNS dari sumber domain yang mungkin belum diklasifikasikan oleh umpan intelijen ancaman yang dikelola oleh komunitas keamanan yang lebih luas.

Saat ini, DNS Firewall Advanced menawarkan perlindungan dari:

- Algoritma Pembuatan Domain () DGAs

DGAs digunakan oleh penyerang untuk menghasilkan sejumlah besar domain untuk meluncurkan serangan malware.

- Terowongan DNS

Tunneling DNS digunakan oleh penyerang untuk mengekstraksi data dari klien dengan menggunakan terowongan DNS tanpa membuat koneksi jaringan ke klien.

- Kamus DGA

Kamus DGAs digunakan oleh penyerang untuk menghasilkan domain menggunakan kata-kata kamus untuk menghindari deteksi dalam komunikasi malware. command-and-control

Untuk mempelajari cara membuat aturan, lihat [Membuat grup aturan dan aturan](#) dan [Pengaturan aturan di DNS Firewall](#).

Mengurangi skenario positif palsu

Jika Anda menghadapi skenario positif palsu dalam aturan yang menggunakan perlindungan DNS Firewall Advanced untuk memblokir kueri, lakukan langkah-langkah berikut:

1. Di log VPC Resolver, identifikasi grup aturan dan proteksi DNS Firewall Advanced yang menyebabkan false positive. Anda melakukan ini dengan menemukan log untuk kueri yang diblokir oleh DNS Firewall, tetapi yang ingin Anda izinkan. Catatan log mencantumkan grup aturan, tindakan aturan, dan perlindungan DNS Firewall Advanced. Untuk informasi lebih lanjut tentang log, lihat [Nilai yang muncul di log kueri VPC Resolver](#).
2. Buat aturan baru di grup aturan yang secara eksplisit mengizinkan kueri yang diblokir. Saat Anda membuat aturan, Anda dapat menentukan daftar domain Anda sendiri hanya dengan spesifikasi domain yang ingin Anda izinkan. Ikuti panduan untuk grup aturan dan manajemen aturan di [Membuat grup aturan dan aturan](#).
3. Prioritaskan aturan baru di dalam grup aturan sehingga berjalan sebelum aturan yang menggunakan daftar terkelola. Untuk melakukan ini, berikan aturan baru pengaturan prioritas numerik yang lebih rendah.

Saat Anda telah memperbarui grup aturan, aturan baru akan secara eksplisit mengizinkan nama domain yang ingin Anda izinkan sebelum aturan pemblokiran berjalan.

Mengonfigurasi pencatatan untuk DNS Firewall

Anda dapat mengevaluasi aturan DNS Firewall Anda dengan menggunakan CloudWatch metrik Amazon dan log kueri Resolver. Log memberikan nama daftar domain untuk semua peringatan dan tindakan pemblokiran. Untuk informasi selengkapnya tentang Amazon CloudWatch, lihat [Memantau grup aturan DNS Firewall Resolver dengan Amazon CloudWatch](#).

Bila Anda mengaktifkan DNS Firewall, kaitkan ke VPC, dan Anda telah log diaktifkan, `firewall_rule_group_id`, `firewall_rule_action`, dan `firewall_domain_list_id` adalah bidang khusus DNS Firewall yang disediakan dalam log Anda.

Note

Log kueri akan menampilkan bidang DNS Firewall tambahan hanya untuk kueri yang diblokir oleh aturan DNS Firewall.

Untuk mulai mencatat kueri DNS yang difilter oleh aturan DNS Firewall yang berasal dari Anda VPCs, Anda melakukan tugas berikut di konsol Amazon Route 53:

Untuk mengonfigurasi pencatatan kueri Resolver untuk DNS Firewall

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Memperluas menu konsol Route 53. Di sudut kiri atas konsol, pilih ikon tiga bilah horizontal ().
3. Dalam menu Resolver, pilih Pencatatan kueri.
4. Di pemilih Region, pilih AWS Wilayah tempat Anda ingin membuat konfigurasi pencatatan kueri.

Ini harus menjadi Wilayah yang sama tempat Anda membuat VPCs yang terkait dengan DNS Firewall yang ingin Anda catat kueri. Jika Anda memiliki VPCs di beberapa Wilayah, Anda harus membuat setidaknya satu konfigurasi pencatatan kueri untuk setiap Wilayah.

5. Pilih Konfigurasi pencatatan kueri.
6. Tentukan nilai-nilai berikut ini:

Nama konfigurasi pencatatan kueri

Masukkan nama untuk konfigurasi pencatatan kueri. Nama muncul di konsol dalam daftar konfigurasi pencatatan kueri. Masukkan nama yang akan membantu Anda menemukan konfigurasi ini nanti.

Tujuan log kueri

Pilih jenis AWS sumber daya yang Anda inginkan VPC Resolver untuk mengirim log kueri. Untuk informasi tentang cara memilih di antara opsi (Grup CloudWatch log log, bucket S3, dan aliran pengiriman Firehose), lihat. [AWS sumber daya yang dapat Anda kirim log kueri VPC Resolver](#)

Setelah Anda memilih jenis sumber daya, Anda dapat membuat sumber daya lain dari jenis itu atau memilih sumber daya yang ada yang dibuat oleh AWS akun saat ini.

 Note

Anda dapat memilih hanya sumber daya yang dibuat di Wilayah AWS yang Anda pilih di langkah 4, Wilayah tempat Anda membuat konfigurasi pencatatan kueri. Jika

Anda memilih untuk membuat sumber daya baru, sumber daya tersebut akan dibuat di Wilayah yang sama.

VPCs untuk mencatat kueri untuk

Konfigurasi pencatatan kueri ini akan mencatat kueri DNS yang berasal dari VPCs yang Anda pilih. Centang kotak untuk setiap VPC di Wilayah saat ini yang Anda inginkan VPC Resolver untuk mencatat kueri, lalu pilih Pilih.

 Note

Pengiriman log VPC hanya dapat diaktifkan sekali untuk jenis tujuan tertentu. Log tidak dapat dikirim ke beberapa tujuan dengan jenis yang sama. Misalnya, log VPC tidak dapat dikirimkan ke dua tujuan Amazon S3.

7. Pilih Configure query logging (Konfigurasi pencatatan kueri).

 Note

Seharusnya Anda mulai melihat kueri DNS yang dibuat oleh sumber daya di VPC Anda di log dalam beberapa menit setelah berhasil membuat konfigurasi pencatatan kueri.

Berbagi grup aturan DNS Firewall Resolver antar akun AWS

Anda dapat berbagi grup aturan DNS Firewall antar AWS akun. Untuk berbagi grup aturan, Anda menggunakan AWS Resource Access Manager (AWS RAM). Konsol DNS Firewall terintegrasi dengan konsol. AWS RAM Untuk informasi selengkapnya AWS RAM, lihat [Panduan Pengguna Resource Access Manager](#).

Perhatikan hal-hal berikut:

Mengaitkan grup aturan bersama dengan VPCs

Jika AWS akun lain telah membagikan grup aturan dengan akun Anda, Anda dapat mengaitkannya dengan cara VPCs yang sama seperti Anda mengaitkan grup aturan yang telah

Anda buat. Untuk informasi selengkapnya, lihat [Mengelola asosiasi antara grup aturan VPC dan Resolver DNS Firewall Anda](#).

Menghapus atau membatalkan berbagi grup aturan bersama

Jika Anda berbagi grup aturan dengan akun lain dan kemudian menghapus grup aturan atau berhenti membagikannya, DNS Firewall menghapus semua asosiasi yang dibuat akun lain antara grup aturan dan grup aturan tersebut. VPCs

Pengaturan maksimum untuk grup aturan dan asosiasi

Grup aturan bersama dan asosiasi VPCs mereka termasuk dalam hitungan untuk akun yang digunakan untuk berbagi grup aturan.

Untuk kuota DNS Firewall saat ini, lihat [Kuota pada Resolver DNS Firewall](#).

Izin

Untuk berbagi grup aturan dengan AWS akun lain, Anda harus memiliki izin untuk menggunakan [PutFirewallRuleGroupPolicy](#) tindakan tersebut.

Pembatasan pada AWS akun tempat grup aturan dibagikan

Akun yang dibagikan grup aturan tidak dapat mengubah atau menghapus grup aturan.

Penandaan

Hanya akun yang membuat grup aturan yang dapat menambahkan, menghapus, atau melihat tanda pada grup aturan.

Untuk melihat status berbagi grup aturan saat ini (termasuk akun yang berbagi grup aturan atau akun yang dibagikan grup aturan), dan untuk berbagi grup aturan dengan akun lain, lakukan prosedur berikut.

Untuk melihat status berbagi dan berbagi grup aturan dengan AWS akun lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Rule groups (Grup aturan).
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat grup aturan.

Kolom Status berbagi menunjukkan status berbagi grup aturan saat ini yang dibuat oleh akun saat ini atau yang dibagikan dengan akun saat ini:

- Tidak dibagikan: AWS Akun saat ini membuat grup aturan, dan grup aturan tidak dibagikan dengan akun lain.
 - Dibagikan oleh saya: Akun saat ini membuat grup aturan dan membagikannya dengan satu atau beberapa akun.
 - Dibagikan dengan saya: Akun saat ini membuat grup aturan dan membagikannya dengan akun saat ini.
4. Pilih nama grup aturan dengan informasi berbagi yang ingin Anda tampilkan atau yang ingin Anda bagikan dengan akun lain.

Pada *rule group name* halaman grup Aturan, nilai di bawah Pemilik menampilkan ID akun yang membuat grup aturan. Itu adalah akun saat ini kecuali nilai Status berbagi adalah Dibagikan dengan saya. Dalam hal ini, Pemilik adalah akun yang membuat grup aturan dan membagikannya dengan akun saat ini.

5. Pilih Share (Bagikan) untuk melihat informasi tambahan atau untuk berbagi grup aturan dengan akun lain. Halaman di AWS IAM konsol muncul, tergantung pada nilai status Berbagi:
- Tidak dibagikan: Halaman Buat berbagi sumber daya akan muncul. Untuk informasi tentang cara berbagi grup aturan dengan akun, unit organisasi (OU), atau organisasi lain, ikuti langkah berikut.
 - Dibagikan oleh saya: Halaman Sumber daya bersama menampilkan grup aturan dan sumber daya lain yang dimiliki oleh akun saat ini dan dibagikan dengan akun lain.
 - Berbagi dengan saya: Halaman Sumber daya bersama menampilkan grup aturan dan sumber daya lain yang dimiliki oleh akun lain dan dibagikan dengan akun saat ini.
6. Untuk berbagi grup aturan dengan AWS akun, OU, atau organisasi lain, tentukan nilai berikut.

 Note

Anda tidak dapat memperbarui pengaturan berbagi. Untuk mengubah salah satu setelan berikut, Anda harus membagikan ulang grup aturan dengan setelan baru, lalu menghapus setelan berbagi yang lama.

Deskripsi

Masukkan deskripsi singkat yang membantu Anda mengingat alasan Anda membagikan grup aturan.

Sumber Daya

Pilih kotak centang untuk grup aturan yang ingin Anda bagikan.

Pengguna utama

Masukkan nomor AWS akun, nama OU, atau nama organisasi.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan pusat Biaya untuk Kunci dan menentukan 456 untuk Nilai.

Ini adalah tag yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda; Anda juga dapat menggunakan tag untuk tujuan lain. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Menggunakan tanda alokasi biaya](#) dalam Panduan Pengguna AWS Billing .

Mengaktifkan perlindungan Resolver DNS Firewall untuk VPC Anda

Anda mengaktifkan perlindungan DNS Firewall untuk VPC Anda dengan mengasosiasikan satu atau beberapa grup aturan dengan VPC. Setiap kali VPC dikaitkan dengan grup aturan DNS Firewall, Route 53 VPC Resolver menyediakan perlindungan DNS Firewall berikut:

- VPC Resolver merutekan kueri DNS keluar VPC melalui DNS Firewall, dan DNS Firewall memfilter kueri menggunakan grup aturan terkait.
- VPC Resolver memberlakukan pengaturan dalam konfigurasi DNS Firewall VPC.

Untuk memberikan perlindungan DNS Firewall untuk VPC Anda, Anda melakukan hal berikut:

- Buat dan kelola asosiasi antara grup aturan DNS Firewall dan VPC Anda. Untuk informasi tentang grup aturan, lihat [Grup aturan dan aturan DNS Firewall](#).
- Konfigurasikan bagaimana Anda ingin VPC Resolver menangani kueri DNS untuk VPC selama kegagalan, misalnya jika DNS Firewall tidak memberikan respons untuk kueri DNS.

Mengelola asosiasi antara grup aturan VPC dan Resolver DNS Firewall Anda

Untuk melihat asosiasi VPC grup aturan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pilih DNS Firewall di panel navigasi untuk membuka halaman grup Aturan Firewall DNS di konsol VPC Amazon.

- ATAU -

Masuk ke Konsol Manajemen AWS dan buka

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

2. Di panel navigasi, di bawah DNS Firewall, pilih Grup aturan.
3. Pada bilah navigasi, pilih Wilayah untuk grup aturan.
4. Pilih grup aturan yang ingin Anda kaitkan.
5. Pilih View details (Lihat detail). Halaman grup aturan ditampilkan.
6. Di bagian bawah, Anda dapat melihat area detail tab yang mencakup aturan dan terkait VPCs. Pilih tab Terkait VPCs.

Mengasosiasikan grup aturan dengan VPC

1. Temukan asosiasi VPC grup aturan dengan mengikuti petunjuk di [prosedur sebelumnya](#) Untuk melihat asosiasi VPC grup aturan.
2. Di VPCs tab Terkait, pilih Associate VPC.
3. Temukan VPC yang ingin Anda kaitkan dengan grup aturan di menu menurun. Pilih, lalu pilih Associate (Kaitkan).

Di halaman grup aturan, VPC Anda tercantum di tab Terkait VPCs. Pada awalnya, laporan Status asosiasi adalah Updating (Memperbarui). Setelah asosiasi selesai, status berubah menjadi Complete (Selesai).

Untuk menghapus asosiasi antara grup aturan dan VPC

1. Temukan asosiasi VPC grup aturan dengan mengikuti petunjuk di [prosedur sebelumnya](#) Untuk melihat asosiasi VPC grup aturan.
2. Pilih VPC yang ingin Anda hapus dari daftar, lalu pilih Disassociate. Verifikasi, dan kemudian konfirmasi tindakan.

Pada halaman grup aturan, VPC Anda tercantum di VPCs tab Terkait dengan status Disassociating. Setelah operasi selesai, DNS Firewall memperbarui daftar untuk menghapus VPC.

Konfigurasi VPC DNS Firewall

Konfigurasi DNS Firewall untuk VPC Anda menentukan apakah Route 53 VPC Resolver memungkinkan kueri melalui atau memblokirnya selama kegagalan, misalnya ketika DNS Firewall terganggu, tidak responsif, atau tidak tersedia di zona. VPC Resolver memberlakukan konfigurasi firewall VPC setiap kali Anda memiliki satu atau lebih grup aturan DNS Firewall yang terkait dengan VPC.

Anda dapat mengonfigurasi VPC agar gagal terbuka atau gagal tertutup.

- Secara default, mode kegagalan ditutup, yang berarti bahwa VPC Resolver memblokir kueri apa pun yang tidak menerima balasan dari DNS Firewall dan mengirimkan respons DNS. SERVFAIL Pendekatan ini mengutamakan keamanan daripada ketersediaan.
- Jika Anda mengaktifkan gagal terbuka, VPC Resolver memungkinkan kueri melalui jika tidak menerima balasan dari DNS Firewall. Pendekatan ini mengutamakan ketersediaan daripada keamanan.

Untuk mengubah konfigurasi DNS Firewall untuk VPC (konsol)

1. Masuk ke Konsol Manajemen AWS dan buka konsol VPC Resolver di. <https://console.aws.amazon.com/route53resolver/>
2. Di panel navigasi di bawah Resolvers, pilih. VPCs
3. Di VPCshalaman, cari dan edit VPC. Ubah konfigurasi DNS Firewall menjadi gagal membuka atau gagal menutup sesuai kebutuhan.

Untuk mengubah perilaku DNS Firewall untuk VPC (API)

- Perbarui konfigurasi firewall VPC Anda dengan memanggil [UpdateFirewallConfig](#) dan mengaktifkan atau menonaktifkan. `FirewallFailOpen`

Anda dapat mengambil daftar konfigurasi firewall VPC Anda melalui API dengan menelepon. [ListFirewallConfigs](#)

Apa itu Profil Amazon Route 53?

Dengan Route 53 Profiles, Anda dapat menerapkan dan mengelola konfigurasi Route 53 terkait DNS di banyak VPCs dan berbeda. Akun AWS Profil membuat pengelolaan pengaturan DNS bagi banyak orang VPCs semudah mengelolanya untuk satu VPC dan ketika Anda memperbarui Profil, pengaturannya disebarkan ke semua VPCs yang terkait dengan Profil. Anda juga dapat berbagi Profil dengan Akun AWS di Wilayah yang sama dengan menggunakan AWS RAM. Sumber daya yang didukung Route 53 saat ini yang dapat Anda kaitkan ke Profil adalah:

- Zona host pribadi dan pengaturan yang ditentukan di dalamnya. Untuk informasi selengkapnya tentang bekerja dengan zona yang dihosting pribadi, lihat [Bekerja dengan zona yang di-hosting privat](#).
- Aturan penyelesai, baik penerusan maupun sistem. Untuk informasi selengkapnya tentang aturan Resolver, lihat [Mengelola aturan penerusan](#).
- Grup aturan DNS Firewall. Untuk informasi selengkapnya tentang grup aturan DNS Firewall, lihat [Grup aturan dan aturan DNS Firewall](#).
- Antarmuka titik akhir VPC. Untuk informasi selengkapnya tentang titik akhir VPC antarmuka, lihat titik akhir [VPC antarmuka di Panduan Pengguna VPC](#) Amazon.
- Konfigurasi pencatatan kueri VPC Resolver. Untuk informasi selengkapnya tentang pencatatan kueri VPC Resolver, lihat [Pencatatan kueri penyelesai](#).

Beberapa konfigurasi VPC dikelola langsung di Profil. Konfigurasinya adalah:

- Membalikkan konfigurasi pencarian DNS untuk Aturan Resolver.
- Konfigurasi mode kegagalan DNS Firewall.
- Konfigurasi validasi DNSSEC.

Misalnya, Anda dapat mengaktifkan konfigurasi mode kegagalan DNS Firewall untuk semua Profil yang VPCs terkait, tetapi pertahankan konfigurasi validasi DNSSEC VPC yang ada.

Important

Setelah Anda mengaktifkan pengaturan Profil untuk konfigurasi sebelumnya, dan mengaitkan Profil ke VPC, pengaturan Profil akan segera berlaku.

Anda juga dapat menggunakan CloudFormation untuk mengatur pengaturan DNS yang konsisten untuk yang baru disediakan VPCs.

Anda dapat mengaitkan satu Profil per VPC dan jumlah sumber daya yang dapat Anda kaitkan per Profil bervariasi. Untuk informasi selengkapnya, lihat [Kuota pada Profil Route 53](#).

Bagaimana pengaturan Route 53 Profil diprioritaskan

Anda dapat mengatur pengaturan dan asosiasi DNS lokal untuk Profil untuk migrasi, atau tujuan pengujian lainnya. Jika kueri DNS cocok dengan aturan Resolver untuk zona host pribadi yang terkait langsung dengan VPC dan aturan Resolver untuk zona host pribadi yang terkait dengan Profil, pengaturan DNS lokal akan diutamakan. Ketika kueri DNS dibuat untuk nama domain yang bertentangan, yang paling spesifik menang. Tabel berikut mencakup contoh urutan evaluasi:

Kueri DNS	Aturan profil	Aturan VPC	Aturan yang dievaluasi
contoh.com	contoh.com	contoh.com	VPC lokal
test.example.com	test.example.com	contoh.com	Profil
pemasaran.example.com	Tidak ada	pemasaran.example.com	VPC lokal

Route 53 Profiles Ketersediaan wilayah

Untuk melihat ketersediaan Wilayah dan titik akhir, lihat [Titik akhir Layanan untuk Rute 53](#) dalam panduan Referensi AWS Umum.

Langkah-langkah tingkat tinggi untuk menggunakan Profil Route 53

Untuk menerapkan Profil Amazon Route 53 di Amazon Virtual Private Cloud VPCs, Anda melakukan langkah-langkah tingkat tinggi berikut.

1. Buat Profil kosong — Langkah pertama adalah membuat Profil kosong tempat Anda dapat mengaitkan sumber daya DNS. Untuk informasi selengkapnya, lihat [Membuat Profil Route 53](#).

2. Mengaitkan sumber daya DNS ke Profil — Sumber daya yang saat ini dapat Anda kaitkan ke Profil adalah zona host pribadi, aturan Resolver, baik penerusan dan sistem, grup aturan DNS Firewall, konfigurasi pencatatan kueri VPC Resolver, dan titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat [Kaitkan grup aturan DNS Firewall dengan Profil Route 53](#), [Kaitkan zona yang di-hosting privat dengan Profil Route 53](#), [Kaitkan aturan Resolver dengan Profil Route 53](#), [Kaitkan konfigurasi pencatatan kueri VPC Resolver ke Profil Route 53](#), dan [Mengaitkan titik akhir VPC antarmuka ke Profil Route 53](#).
3. Konfigurasi beberapa pengaturan VPC untuk Profil — Beberapa pengaturan DNS, seperti zona yang dihosting yang terkait dengan Profil, diterapkan segera. VPCs Untuk validasi DNSSEC, Resolver reverse DNS lookup, dan konfigurasi mode kegagalan DNS Firewall, Anda dapat memilih salah satu opsi berikut:
 - Untuk validasi DNSSEC, Anda dapat memilih untuk menggunakan konfigurasi VPC lokal (default), mengaktifkan validasi, atau menonaktifkan validasi untuk semua yang terkait dengan Profil. VPCs
 - Untuk konfigurasi pencarian DNS balik Resolver, Anda dapat mengaktifkannya, menonaktifkannya, atau menggunakan aturan yang ditentukan secara otomatis yang ditentukan untuk VPC secara lokal (default).
 - Untuk konfigurasi mode kegagalan DNS Firewall Anda dapat mengaktifkannya, menonaktifkannya, atau menggunakan konfigurasi mode kegagalan yang ditentukan untuk VPC secara lokal (default).

Untuk informasi selengkapnya, lihat [Edit Route 53 Konfigurasi profil](#).

4. Kaitkan Profil dengan satu atau lebih VPCs — Untuk mulai menggunakan Profil Anda, kaitkan dengan satu atau lebih VPCs. Untuk informasi selengkapnya, lihat [Kaitkan Profil Route 53 ke VPCs](#).

Membuat Profil Route 53

Untuk membuat Profil Route 53, ikuti panduan dalam topik ini. Pilih tab untuk membuat Profil Route 53 menggunakan konsol Route 53, atau AWS CLI.

- [Konsol](#)
- [CLI](#)

Console

Untuk membuat Profil Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pada bilah navigasi, pilih Wilayah tempat Anda ingin membuat Profil.
4. Masukkan nama untuk Profil, tambahkan tag secara opsional, dan pilih Buat Profil.

Ini membuat Profil kosong dengan konfigurasi default yang dapat Anda kaitkan sumber daya. Setelah Anda mengaitkan sumber daya ke Profil, Anda dapat mengaitkannya ke sejumlah VPCs dan mengedit bagaimana beberapa konfigurasi Resolver berlaku untuk VPCs

CLI

Anda dapat membuat Profil dengan menjalankan AWS CLI perintah seperti berikut dan menggunakan nilai Anda sendiri untuk `username`.

```
aws route53profiles create-profile --name test
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "Profile": {
    "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
    "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
    "CreationTime": 1710850903.578,
    "Id": "rp-6ffe47d5example",
    "ModificationTime": 1710850903.578,
    "Name": "test",
    "OwnerId": "123456789012",
    "ShareStatus": "NOT_SHARED",
    "Status": "COMPLETE",
    "StatusMessage": "Created Profile"
  }
}
```

Untuk mengaitkan Profil Anda dengan sumber daya yang berbeda dan mengedit konfigurasi VPC untuk Profil, lihat prosedur berikut:

Topik

- [Kaitkan grup aturan DNS Firewall dengan Profil Route 53](#)
- [Kaitkan zona yang di-hosting privat dengan Profil Route 53](#)
- [Kaitkan aturan Resolver dengan Profil Route 53](#)
- [Mengaitkan titik akhir VPC antarmuka ke Profil Route 53](#)
- [Kaitkan konfigurasi pencatatan kueri VPC Resolver ke Profil Route 53](#)
- [Edit Route 53 Konfigurasi profil](#)
- [Kaitkan Profil Route 53 ke VPCs](#)

Kaitkan grup aturan DNS Firewall dengan Profil Route 53

Untuk petunjuk membuat grup aturan, lihat [Membuat grup aturan dan aturan](#), lalu pilih tab untuk mengaitkan grup aturan DNS Firewall ke Profil Route 53 menggunakan konsol Route 53, atau AWS CLI.

- [Konsol](#)
- [CLI](#)

Console

Untuk mengaitkan grup aturan DNS Firewall

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
3. Di panel navigasi, pilih Profil dan pada tabel Profil, pilih nama yang ditautkan dari Profil yang ingin Anda gunakan.
4. Pada <Profile name>halaman, pilih tab grup aturan DNS Firewall dan kemudian Associate.
5. Di bagian grup aturan DNS Firewall, Anda dapat memilih hingga 10 grup aturan yang telah Anda buat sebelumnya. Jika Anda ingin mengaitkan lebih dari 10 grup aturan, gunakan APIs. Untuk informasi selengkapnya, lihat [AssociateResourceToProfile](#).

Untuk membuat grup aturan baru, lihat [Membuat grup aturan dan aturan](#).

6. Pilih Berikutnya.
7. Pada halaman Tentukan prioritas, Anda dapat mengatur urutan grup aturan diproses dengan mengklik nomor prioritas yang telah ditetapkan sebelumnya dan mengetikkan yang baru. Nilai yang diizinkan untuk prioritas adalah antara 100 dan 9900.

Grup aturan dievaluasi dimulai dengan pengaturan prioritas numerik terendah dan naik. Anda dapat mengubah prioritas grup aturan kapan saja, misalnya untuk mengubah urutan pemrosesan atau membuat ruang untuk grup aturan lainnya.

Pilih Kirim.

8. Kemajuan asosiasi ditampilkan di kolom Status di kotak dialog grup aturan DNS Firewall.

CLI

Anda dapat mengaitkan grup aturan ke Profil dengan menjalankan AWS CLI perintah seperti berikut ini dan menggunakan nilai Anda sendiri untuk `nameprofile-id`, `resource-arn`, dan `priority`:

```
aws route53profiles associate-resource-to-profile --name test-resource-association --profile-id rp-4987774726example --resource-arn arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example --resource-properties '{"priority": 102}'
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "ProfileResourceAssociation": {
    "CreationTime": 1710851216.613,
    "Id": "rpr-001913120a7example",
    "ModificationTime": 1710851216.613,
    "Name": "test-resource-association",
    "OwnerId": "123456789012",
    "ProfileId": "rp-4987774726example",
    "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example",
    "ResourceProperties": '{"priority":102}',
    "ResourceType": "FIREWALL_RULE_GROUP",
    "Status": "UPDATING",
```

```
"StatusMessage": "Updating the Profile to DNS Firewall rule group  
association"  
}  
}
```

Kaitkan zona yang di-hosting privat dengan Profil Route 53

Untuk intruksi tentang cara membuat zona host pribadi, lihat [Membuat zona yang di-hosting privat](#), lalu ikuti langkah-langkah dalam prosedur ini untuk mengaitkan zona host pribadi ke Profil.

Untuk mengaitkan zona yang dihosting pribadi

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
3. Di panel navigasi, pilih Profil dan pada tabel Profil, pilih nama yang ditautkan dari Profil yang ingin Anda gunakan.
4. Pada <Profile name>halaman, pilih tab Zona yang dihosting pribadi, lalu Kaitkan.
5. Pada halaman Associate private hosted zones, Anda dapat memilih hingga 10 zona host pribadi yang telah Anda buat sebelumnya. Jika Anda ingin mengaitkan lebih dari 10 zona yang dihosting pribadi, gunakan APIs. Untuk informasi selengkapnya, lihat [AssociateResourceToProfile](#).

Untuk membuat zona yang dihosting pribadi, lihat [Membuat zona yang di-hosting privat](#).

6. Pilih Associate
7. Kemajuan asosiasi ditampilkan di kolom Status pada tab Zona yang dihosting pribadi.

Kaitkan aturan Resolver dengan Profil Route 53

Untuk petunjuk cara membuat aturan Resolver, lihat [Membuat aturan penerusan](#), lalu ikuti langkah-langkah dalam prosedur ini untuk mengaitkan aturan Resolver ke Profil.

Untuk mengaitkan aturan Resolver VPC

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.

3. Pada halaman, pilih tab Aturan Resolver, lalu Kaitkan. <Profile name>
4. Pada halaman Aturan Resolver Associate, di tabel aturan Resolver Anda dapat memilih hingga 10 aturan Resolver yang telah Anda buat sebelumnya. Jika Anda ingin mengaitkan lebih dari 10 aturan resolver, gunakan. APIs Untuk informasi selengkapnya, lihat [AssociateResourceToProfile](#).

Untuk membuat aturan Resolver, lihat. [Membuat aturan penerusan](#)

5. Pilih Associate
6. Kemajuan asosiasi ditampilkan di kolom Status pada aturan Resolver tab.

Mengaitkan titik akhir VPC antarmuka ke Profil Route 53

Untuk petunjuk tentang cara membuat titik akhir VPC antarmuka, lihat Membuat titik akhir [VPC di Panduan Pengguna VPC](#). dan kemudian ikuti langkah-langkah dalam prosedur ini untuk mengaitkan titik akhir VPC ke Profil.

Untuk mengaitkan titik akhir VPC

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
3. Pada halaman, pilih tab titik akhir VPC, lalu Associate. <Profile name>
4. Pada halaman titik akhir VPC Associate, di tabel titik akhir VPC Anda dapat memilih hingga 10 titik akhir yang telah Anda buat sebelumnya. Jika Anda ingin mengaitkan lebih dari 10 titik akhir, gunakan. APIs Untuk informasi selengkapnya, lihat [AssociateResourceToProfile](#).

Untuk membuat aturan Resolver, lihat. [Membuat aturan penerusan](#)

5. Pilih Associate
6. Kemajuan asosiasi ditampilkan di kolom Status pada titik akhir VPC tab.

Kaitkan konfigurasi pencatatan kueri VPC Resolver ke Profil Route 53

Untuk petunjuk tentang cara membuat konfigurasi logging kueri VPC Resolver, lihat [Mengkonfigurasi \(pencatatan kueri VPC Resolver\)](#), lalu pilih tab untuk mengaitkan konfigurasi Resolver VPC ke Profil Route 53 menggunakan konsol Route 53, atau. AWS CLI

- [Konsol](#)

- [CLI](#)

Console

Untuk mengaitkan konfigurasi pencatatan kueri

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
3. Pada halaman Nama profil, pilih tab konfigurasi log kueri Resolver, lalu Kaitkan.
4. Pada halaman Konfigurasi pencatatan kueri asosiasi, di tabel konfigurasi log kueri Resolver, Anda dapat memilih hingga tiga konfigurasi yang sebelumnya Anda buat. Jika Anda ingin mengaitkan lebih dari tiga konfigurasi pencatatan kueri, gunakan API. Untuk informasi selengkapnya, lihat [AssociateResourceToProfile](#).
5. Untuk membuat konfigurasi logging kueri VPC Resolver baru, lihat. [Mengkonfigurasi \(pencatatan kueri VPC Resolver\)](#)
6. Pilih Associate
7. Kemajuan asosiasi ditampilkan di kolom Status pada konfigurasi log kueri Resolver tab.

CLI

Anda dapat mengaitkan konfigurasi log kueri ke Profil dengan menjalankan AWS CLI perintah seperti berikut ini dan menggunakan nilai Anda sendiri untuk name profile-id dan resource-arn.

```
aws route53profiles associate-resource-to-profile --name test-resource-association --profile-id rp-4987774726example --resource-arn arn:aws:route53resolver:us-east-1:123456789012:resolver-query-log-config/rqlc-cfe7f72example
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "ProfileResourceAssociation": {
    "CreationTime": 1710851226.613,
    "Id": "rpr-001913120b8example",
    "ModificationTime": 1710851226.613,
    "Name": "test-resource-association",
```

```
{
  "OwnerId": "123456789012",
  "ProfileId": "rp-4987774726example",
  "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:resolver-
query-log-config/rqlc-cfe7f72example",
  "ResourceType": "RESOLVER_QUERY_LOG_CONFIG",
  "Status": "CREATING",
  "StatusMessage": "Creating rp-4987774726example to rqlc-cfe7f72example
association"
}
```

Edit Route 53 Konfigurasi profil

Setelah Anda mengaitkan sumber daya ke Profil, Anda dapat mengedit konfigurasi VPC default untuk memutuskan bagaimana mereka diterapkan ke VPCs

Untuk mengedit konfigurasi Profil

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
3. Di panel navigasi, pilih Profil dan pada tabel Profil, pilih nama yang ditautkan dari Profil yang ingin Anda gunakan.
4. Pada <Profile name>halaman, pilih tab Konfigurasi dan kemudian Edit.
5. Pada halaman Edit Konfigurasi, pilih salah satu nilai untuk konfigurasi DNSSEC VPC, konfigurasi pencarian DNS terbalik Resolver, dan konfigurasi mode kegagalan DNS Firewall.

Untuk informasi selengkapnya tentang nilai, lihat [Pengaturan konfigurasi untuk Profil Route 53](#).

6. Pilih Perbarui.

Pengaturan konfigurasi untuk Profil Route 53

Saat Anda mengedit konfigurasi Profil Route 53, Anda menentukan nilai berikut:

Konfigurasi DNSSEC

Pilih salah satu nilai berikut:

- Gunakan konfigurasi DNSSEC VPC lokal - default

Pilih opsi ini agar semua yang VPCs terkait dengan Profil ini menyimpan konfigurasi validasi DNSSEC lokal mereka.

- Mengaktifkan validasi DNSSEC

Pilih opsi ini untuk mengaktifkan validasi DNSSEC di semua yang VPCs terkait dengan Profil ini.

- Nonaktifkan validasi DNSSEC

Pilih opsi ini untuk menonaktifkan validasi DNSSEC di semua VPCs yang terkait dengan Profil ini.

Konfigurasi pencarian DNS terbalik Resolver

Pilih salah satu nilai berikut:

- Aktifkan

Pilih opsi ini untuk membuat aturan yang ditentukan secara otomatis untuk pencarian DNS terbalik di semua yang terkait VPCs.

- Tidak diaktifkan

Pilih opsi ini untuk tidak membuat aturan yang ditentukan secara otomatis untuk pencarian DNS terbalik di semua yang terkait VPCs.

- Gunakan aturan yang ditentukan otomatis lokal - default

Pilih opsi ini untuk menggunakan pengaturan VPC lokal untuk pencarian DNS terbalik untuk yang terkait. VPCs

Konfigurasi mode kegagalan DNS Firewall

Pilih salah satu nilai berikut:

- Nonaktifkan

Pilih opsi ini untuk menutup mode kegagalan DNS Firewall untuk yang terkait VPCs. Dengan opsi ini, DNS Firewall akan memblokir semua kueri yang tidak dapat dievaluasi dengan benar.

- Diaktifkan

Pilih opsi ini untuk menjaga mode kegagalan DNS Firewall tetap terbuka untuk semua yang terkait VPCs. Dengan opsi ini, DNS Firewall akan memungkinkan kueri untuk melanjutkan jika tidak dapat mengevaluasi mereka dengan benar.

- Gunakan pengaturan mode kegagalan lokal - default

Pilih opsi ini untuk menggunakan pengaturan mode kegagalan VPC DNS Firewall lokal.

Untuk informasi selengkapnya tentang konfigurasi, lihat

- [Mengaktifkan validasi DNSSEC di Amazon Route 53](#)
- [Aturan penerusan untuk kueri DNS terbalik di VPC Resolver](#)
- [Konfigurasi VPC DNS Firewall](#)

Kaitkan Profil Route 53 ke VPCs

Untuk mengaitkan Profil Route 53 ke VPC, ikuti panduan dalam topik ini. Pilih tab untuk mengaitkan Profil Route 53 ke VPC menggunakan konsol Route 53, atau. AWS CLI

- [Konsol](#)
- [CLI](#)

Console

Untuk mengasosiasikan VPCs

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
3. Pada <Profile name>halaman, pilih VPCstab, dan kemudian Associate.
4. Pada VPCs halaman Associate Anda dapat memilih hingga 10 yang telah VPCs Anda buat sebelumnya. Jika Anda ingin mengasosiasikan lebih dari 10 VPCs, gunakan APIs. Untuk informasi selengkapnya, lihat [AssociateProfile](#).
5. Pilih Associate
6. Kemajuan asosiasi ditampilkan di kolom Status pada VPCshalaman.

CLI

Anda dapat membuat daftar Profil dengan menjalankan AWS CLI perintah seperti berikut ini dan menggunakan nilai Anda sendiri untuk `username`, `profile-id`, dan `resource-id`:

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "ProfileResourceAssociation": {
    "CreationTime": 1710851216.613,
    "Id": "rpr-001913120a7example",
    "ModificationTime": 1710851216.613,
    "Name": "test-resource-association",
    "OwnerId": "123456789012",
    "ProfileId": "rp-4987774726example",
    "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example",
    "ResourceProperties": "{\"priority\":102}",
    "ResourceType": "FIREWALL_RULE_GROUP",
    "Status": "UPDATING",
    "StatusMessage": "Updating the Profile to DNS Firewall rule group association"
  }
}
```

Melihat dan memperbarui Profil Amazon Route 53

Pilih tab konsol untuk melihat dan mengedit Profil Route 53. Pilih tab CLI yang akan digunakan AWS CLI untuk mencantumkan Profil yang Anda miliki, dibagikan oleh Anda, atau dibagikan kepada Anda.

- [Konsol](#)
- [CLI](#)

Console

Melihat dan memperbarui Profil Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pilih tombol di sebelah nama Profil yang ingin Anda lihat atau edit.

4. Pada <Profile name>halaman Anda dapat melihat sumber daya DNS yang saat ini terkait, mengaitkan yang baru, dan mengedit tag dan konfigurasi VPC.

CLI

Anda dapat membuat daftar Profil dengan menjalankan AWS CLI perintah seperti berikut:

```
aws route53profiles list-profiles
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "ProfileSummaries": [
    {
      "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
      "Id": "rp-4987774726example",
      "Name": "test",
      "ShareStatus": "NOT_SHARED"
    }
  ]
}
```

Anda bisa mendapatkan informasi tentang VPS tertentu yang terkait dengan Profil dengan menjalankan AWS CLI perintah seperti berikut dan menggunakan nilai Anda sendiri untuk `profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
"ProfileAssociation": {
  "CreationTime": 1709338817.148,
  "Id": "rrpassoc-489ce212fexample",
  "ModificationTime": 1709338974.772,
  "Name": "test-association",
  "OwnerId": "123456789012",
  "ProfileId": "rp-4987774726example",
  "ResourceId": "vpc-0af3b96b3example",
  "Status": "COMPLETE",
```

```
    "StatusMessage": "Created Profile Association"  
  }  
]  
}
```

Menghapus Profil Amazon Route 53

Pilih tab untuk menghapus Profil Route 53 menggunakan konsol Route 53, atau AWS CLI.

- [Konsol](#)
- [CLI](#)

Console

Untuk menghapus Profil Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pilih tombol di sebelah nama Profil yang ingin Anda hapus, lalu pilih Hapus.

Important

Anda tidak dapat menghapus Profil jika dikaitkan dengan VPCs. Selain itu, jika Profil dibagikan ke yang lain Akun AWS, konfigurasi Profil apa pun VPCs yang terkait dengan konfigurasi Profil, akan kehilangan konfigurasi tersebut.

4. Pada <Profile name>dialog Hapus, ketik **confirm**, lalu pilih Hapus.

CLI

Important

Anda tidak dapat menghapus Profil jika dikaitkan dengan VPCs. Selain itu, jika Profil dibagikan ke yang lain Akun AWS, konfigurasi Profil apa pun VPCs yang terkait dengan konfigurasi Profil, akan kehilangan konfigurasi tersebut.

Anda dapat menghapus Profil dengan menjalankan AWS CLI perintah seperti berikut dan menggunakan nilai Anda sendiri untuk `profile-id`:

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "Profile": {
    "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
    "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
    "CreationTime": 1710850903.578,
    "Id": "rp-6ffe47d5example",
    "ModificationTime": 1710850903.578,
    "Name": "test",
    "OwnerId": "123456789012",
    "ShareStatus": "NOT_SHARED",
    "Status": "DELETED",
    "StatusMessage": "Deleted Profile"
  }
}
```

Melihat dan memperbarui sumber daya Route 53 yang terkait dengan Profil Amazon Route 53

Pilih tab konsol untuk melihat asosiasi sumber daya Profil Route 53, dan secara opsional mengedit prioritas grup aturan DNS Firewall. Pilih tab CLI yang akan digunakan AWS CLI untuk daftar asosiasi sumber daya dan untuk melihat contoh pembaruan ke prioritas grup aturan DNS Firewall.

- [Konsol](#)
- [CLI](#)

Console

Untuk melihat dan memperbarui sumber daya yang terkait dengan Profil

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

2. Di panel navigasi, pilih Profil.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
4. Pilih tombol di sebelah nama Profil yang ingin Anda lihat atau edit asosiasi sumber daya.
5. Pada halaman pilih tab untuk sumber daya yang ingin Anda lihat atau edit, baik, grup aturan DNS Firewall, Zona yang dihosting pribadi, aturan Resolver, atau titik akhir VPC. <Profile name>
6. Pada halaman tab untuk sumber daya Anda dapat melihat nama, ARN dan status untuk sumber daya terkait. Anda juga dapat memilih ikon roda gigi untuk menyesuaikan apa yang ditampilkan di tabel sumber daya.

Pada halaman tab grup aturan DNS Firewall, Anda juga dapat memilih entri prioritas grup aturan, dan mengeditnya ke angka yang lebih kecil atau lebih besar. Kelompok aturan dievaluasi secara berurutan mulai dari nomor prioritas terendah hingga nomor prioritas tertinggi.

CLI

Anda dapat membuat daftar sumber daya yang terkait dengan Profil dengan menjalankan AWS CLI perintah seperti berikut ini dan menggunakan nilai Anda sendiri untuk `profile-id`:

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "ProfileResourceAssociations": [
    {
      "CreationTime": 1710851216.613,
      "Id": "rpr-001913120a7example",
      "ModificationTime": 1710851216.613,
      "Name": "test-resource-association",
      "OwnerId": "123456789012",
      "ProfileId": "rp-4987774726example",
      "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
      "ResourceProperties": "{\"priority\":102}",
      "ResourceType": "FIREWALL_RULE_GROUP",
      "Status": "COMPLETE",
```

```

        "StatusMessage": "Completed creation of Profile to DNS Firewall rule
group association"
    }
]
}

```

Anda dapat memperbarui prioritas grup aturan DNS Firewall yang terkait dengan Profil dengan menjalankan AWS CLI perintah seperti berikut ini dan menggunakan nilai Anda sendiri untuk `profile-resource-association-id` dan `--resource-properties`:

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```

{
  "ProfileResourceAssociation": {
    "CreationTime": 1710851216.613,
    "Id": "rpr-001913120a7example",
    "ModificationTime": 1710852303.798,
    "Name": "test-resource-association",
    "OwnerId": "123456789012",
    "ProfileId": "rp-4987774726example",
    "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
    "ResourceProperties": "{\"priority\":105}",
    "ResourceType": "FIREWALL_RULE_GROUP",
    "Status": "UPDATING",
    "StatusMessage": "Updating the Profile to DNS Firewall rule group
association"
  }
}

```

Memutuskan sumber daya dari Profil Amazon Route 53

Sebelum Anda menghapus Profil, Anda harus memisahkan semua sumber daya darinya.

Untuk memisahkan sumber daya yang terkait dengan Profil Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pada bilah navigasi, pilih Wilayah tempat Profil tempat Anda ingin memisahkan sumber daya dibuat.
4. Pilih tombol di sebelah nama Profil tempat Anda ingin memisahkan sumber daya.
5. Pada halaman Nama profil pilih tab untuk sumber daya yang ingin Anda hapus, baik, grup aturan DNS Firewall, Zona yang dihosting pribadi, Pencatatan kueri Resolver, aturan Resolver, atau titik akhir VPC.
6. Pada halaman tab untuk sumber daya, pilih sumber daya yang ingin Anda pisahkan dan kemudian Putuskan.
7. Dalam dialog Disassociate resource, ketik **confirm**, lalu pilih Disassociate.

Melihat VPCs terkait dengan Profil Amazon Route 53

Pilih tab konsol untuk melihat dan mengedit Profil Route 53 ke asosiasi VPC. Pilih tab CLI yang akan digunakan untuk mencantumkan Profil AWS CLI ke asosiasi VPC, atau untuk mendapatkan informasi tentang asosiasi tertentu

- [Konsol](#)
- [CLI](#)

Console

Untuk melihat VPCs terkait dengan Profil

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat Profil.
4. Pilih tombol di sebelah nama Profil yang ingin Anda lihat terkait VPCs.
5. Pada <Profile name>halaman pilih VPCstab.

6. Pada halaman tab untuk VPCs Anda dapat melihat nama, ARN dan status untuk yang terkait. VPCs

CLI

Anda dapat membuat daftar Profil terkait dengan menjalankan AWS CLI perintah seperti berikut: VPCs

```
aws route53profiles list-profile-associations
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
{
  "ProfileAssociations": [
    {
      "CreationTime": 1709338817.148,
      "Id": "rpassoc-489ce212fexample",
      "ProfileAssociations": [
        {
          "CreationTime": 1709338817.148,
          "Id": "rpassoc-489ce212fexample",
          "ModificationTime": 1709338974.772,
          "Name": "test-association",
          "OwnerId": "123456789012",
          "ProfileId": "rp-4987774726example",
          "ResourceId": "vpc-0af3b96b3example",
          "Status": "COMPLETE",
          "StatusMessage": "Created Profile Association"
        }
      ]
    }
  ],
  "ModificationTime": 1709338974.772,
  "Name": "test-association",
  "OwnerId": "123456789012",
  "ProfileId": "rp-4987774726example",
  "ResourceId": "vpc-0af3b96b3example",
  "Status": "COMPLETE",
  "StatusMessage": "Created Profile Association"
}
```

Anda bisa mendapatkan informasi tentang VPS tertentu yang terkait dengan Profil dengan menjalankan AWS CLI perintah seperti berikut dan menggunakan nilai Anda sendiri untuk `profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id  
rrpassoc-489ce212fexample
```

Berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
"ProfileAssociation": {  
  "CreationTime": 1709338817.148,  
  "Id": "rrpassoc-489ce212fexample",  
  "ModificationTime": 1709338974.772,  
  "Name": "test-association",  
  "OwnerId": "123456789012",  
  "ProfileId": "rp-4987774726example",  
  "ResourceId": "vpc-0af3b96b3example",  
  "Status": "COMPLETE",  
  "StatusMessage": "Created Profile Association"  
}
```

Memutuskan VPC dari Profil Amazon Route 53

Pilih tab untuk memisahkan Profil Route 53 dari VPC menggunakan konsol Route 53, atau. AWS CLI

- [Konsol](#)
- [CLI](#)

Console

Untuk memisahkan VPC yang terkait dengan Profil Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pada bilah navigasi, pilih Wilayah tempat Profil tempat Anda ingin memisahkan VPC dibuat.
4. Pilih tombol di sebelah nama Profil tempat Anda ingin memisahkan VPC.

5. Pada <Profile name>halaman pilih VPCstab.
6. Pada halaman VPCs tab untuk sumber daya, pilih VPC yang ingin Anda pisahkan dan kemudian Putuskan.
7. Dalam dialog Disassociate resource, ketik**confirm**, lalu pilih Disassociate.

CLI

Anda dapat memisahkan Profil dari VPC dengan menjalankan AWS CLI perintah seperti berikut dan menggunakan nilai Anda sendiri untuk `profile-id` dan `resource-id`:

```
aws route53profiles disassociate-profile --profile-id  
rp-4987774726example --resource-id vpc-0af3b96b3example
```

berikut ini adalah contoh output setelah Anda menjalankan perintah:

```
"ProfileAssociation": {  
  "CreationTime": 1710851336.527,  
  "Id": "rpassoc-489ce212fexample",  
  "ModificationTime": 1710851401.362,  
  "Name": "test-association",  
  "OwnerId": "123456789012",  
  "ProfileId": "rp-4987774726example",  
  "ResourceId": "vpc-0af3b96b3example",  
  "Status": "DELETING",  
  "StatusMessage": "Deleting Profile Association"  
}
```

Bekerja dengan Profil Route 53 bersama

Anda dapat berbagi Profil dengan akun lain dengan:

- Memberikan izin hanya-baca, yang berarti akun lain dapat mengaitkan Profil dengan profil mereka. VPCs Dalam hal ini semua sumber daya dan konfigurasi DNS akan berlaku pada yang terkait. VPCs
- Memberikan izin admin. Dalam hal ini akun dengan Profil bersama dapat mengubah Profil dan kemudian mengaitkannya dengan profil mereka VPCs. Pemilik juga dapat membuat izin terkelola pelanggan yang dapat digunakan untuk menentukan tindakan mana yang dapat dilakukan oleh

akun konsumen. Untuk informasi selengkapnya, lihat [Izin terkelola pelanggan](#) di Panduan AWS RAM Pengguna.

Profil Amazon Route 53 terintegrasi dengan AWS Resource Access Manager (AWS RAM) untuk mengaktifkan berbagi sumber daya. AWS RAM adalah layanan yang memungkinkan Anda untuk berbagi beberapa sumber daya Route 53 dengan yang lain Akun AWS atau melalui AWS Organizations. Dengan AWS RAM, Anda berbagi sumber daya yang Anda miliki dengan membuat pembagian sumber daya. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat mencakup:

- Spesifik Akun AWS
- Unit organisasi di dalam organisasinya di AWS Organizations
- Seluruh organisasinya di AWS Organizations

Untuk informasi selengkapnya AWS RAM, lihat [Panduan AWS RAM Pengguna](#).

Topik ini menjelaskan cara berbagi sumber daya yang Anda miliki, dan cara menggunakan sumber daya yang dibagikan dengan Anda.

Daftar Isi

- [Memberikan izin untuk berbagi Profil Route 53](#)
- [Prasyarat untuk berbagi Profil Route 53](#)
- [Berbagi Profil Route 53](#)
- [Membatalkan berbagi Profil Route 53 bersama](#)
- [Mengidentifikasi Profil Route 53 bersama](#)
- [Tanggung jawab dan izin untuk Profil Route 53 bersama](#)
- [Tagihan dan pengukuran](#)
- [Kuota contoh](#)

Memberikan izin untuk berbagi Profil Route 53

Satu set izin minimum diperlukan untuk kepala sekolah IAM untuk berbagi Profil. Sebaiknya gunakan kebijakan IAM `AmazonRoute53ProfilesFullAccess` terkelola untuk memastikan kepala sekolah IAM Anda memiliki izin yang diperlukan untuk berbagi dan menggunakan Profil bersama.

Jika Anda menggunakan kebijakan IAM kustom, `route53profiles:PutProfilePolicy` tindakan `route53profiles:GetProfilePolicy` dan tindakan diperlukan. Ini adalah tindakan IAM khusus izin. Jika kepala sekolah IAM tidak memiliki izin ini diberikan, kesalahan akan terjadi saat mencoba membagikan Profil menggunakan layanan. AWS RAM

Prasyarat untuk berbagi Profil Route 53

- Untuk membagikan Profil Route 53, Anda harus memilikinya di profil Anda Akun AWS. Ini berarti bahwa sumber daya harus dialokasikan atau disediakan di akun Anda. Anda tidak dapat membagikan Profil Route 53 yang telah dibagikan kepada Anda.
- Untuk berbagi Profil Route 53 dengan organisasi Anda atau unit organisasi di AWS Organizations, Anda harus mengaktifkan berbagi dengan AWS Organizations. Untuk informasi selengkapnya, lihat [Mengaktifkan Berbagi dengan AWS Organizations](#) di Panduan AWS RAM Pengguna.

Berbagi Profil Route 53

Ketika Anda berbagi Profil yang Anda miliki dengan orang lain Akun AWS, Anda memungkinkan mereka untuk menerapkan pengaturan terkait DNS dari Profil ke profil mereka. VPCs Ini membuatnya lebih mudah untuk menerapkan konfigurasi DNS seragam di ribuan VPCs dengan overhead manajemen minimal.

Untuk membagikan Profil Route 53, Anda harus menambahkannya ke berbagi sumber daya. Pembagian sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya Anda Akun AWS. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan berbagi dengan mereka. Saat membagikan Profil Route 53 menggunakan konsol Route 53, Anda menambahkannya ke pembagian sumber daya yang ada. Untuk menambahkan Profil Route 53 ke pembagian sumber daya baru, Anda harus terlebih dahulu membuat pembagian sumber daya menggunakan [AWS RAM konsol](#).

Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda secara otomatis diberikan akses ke Profil Route 53 bersama. Jika tidak, konsumen menerima undangan untuk bergabung dengan pembagian sumber daya dan diberikan akses ke Profil Route 53 bersama setelah menerima undangan.

Anda dapat mulai membagikan Profil Route 53 yang Anda miliki di konsol Route 53 dan melanjutkan di AWS RAM konsol.

Untuk membagikan Profil Route 53 yang Anda miliki menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pilih Profil yang ingin Anda bagikan, dan pada halaman Detail profil, pilih Bagikan profil.
4. Anda dibawa ke AWS RAM konsol tempat Anda dapat mengikuti langkah-langkah berikut: [Membuat Pembagian Sumber Daya](#) di Panduan AWS RAM Pengguna.
5. Jika Profil dibagikan kepada Anda, tabel Profil menyertakan teks yang Dibagikan dengan saya.

Ketika Anda telah berbagi Profil, itu terdaftar sebagai Dibagikan dalam tabel Profil.

Untuk membagikan Profil Route 53 yang Anda miliki menggunakan AWS RAM konsol

Lihat [Membuat Sumber Daya Bersama](#) di Panduan Pengguna AWS RAM .

Untuk membagikan Profil Route 53 yang Anda miliki menggunakan AWS CLI

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

Membatalkan berbagi Profil Route 53 bersama

Ketika Anda membatalkan pembagian Profil, dan VPCs yang memiliki konfigurasi Profil yang terkait dengannya, akan kehilangannya, dan default ke konfigurasi khusus VPC.

Untuk membatalkan berbagi Profil Route 53 bersama yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini menggunakan konsol Route 53, AWS RAM konsol, atau AWS CLI.

Untuk membatalkan pembagian Profil Route 53 bersama yang Anda miliki menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Pilih nama yang ditautkan dari Profil yang ingin Anda batalkan, dan pada <Profile name>halaman, pilih Kelola berbagi.

4. Anda dibawa ke AWS RAM konsol tempat Anda dapat mengikuti langkah-langkah berikut:
[Memperbarui Pembagian Sumber Daya](#) di Panduan AWS RAM Pengguna.

Untuk membatalkan berbagi Profil Route 53 bersama yang Anda miliki menggunakan konsol AWS RAM

Lihat [Memperbarui Sumber Daya Bersama](#) di Panduan Pengguna AWS RAM .

Untuk membatalkan pembagian Profil Route 53 bersama yang Anda miliki menggunakan AWS CLI

Gunakan perintah [disassociate-resource-share](#).

Mengidentifikasi Profil Route 53 bersama

Pemilik dan konsumen dapat mengidentifikasi Profil Route 53 bersama menggunakan konsol Route 53 dan AWS CLI.

Untuk mengidentifikasi Profil Route 53 bersama menggunakan konsol Route 53

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Profil.
3. Jika Profil dibagikan kepada Anda, tabel Profil menyertakan teks yang Dibagikan dengan saya.

Ketika Anda telah berbagi Profil, itu terdaftar sebagai Dibagikan dalam tabel Profil.

Untuk mengidentifikasi Profil Route 53 bersama menggunakan AWS CLI

Gunakan perintah [get-profile](#) atau [list-profile](#). Perintah menampilkan informasi tentang Profil Route 53 yang Anda miliki dan status berbagi Profil Route 53.

Tanggung jawab dan izin untuk Profil Route 53 bersama

Izin untuk pemilik

Pemilik Profil dapat melihat, mengelola, dan menghapus Asosiasi sumber daya Profil, termasuk asosiasi sumber daya yang dibuat oleh akun konsumen. Pemilik dapat melihat dan menghapus asosiasi VPC yang mereka miliki. Selain itu, hanya pemilik Profil yang dapat menghapus Profil yang mereka miliki, dan ini juga secara otomatis menghapus semua asosiasi sumber daya Profil.

 Note

Anda harus membuat izin terkelola khusus yang menyertakan `route53profiles:AssociateResourceToProfile` tindakan selain yang default untuk mengaitkan sumber daya apa pun dari akun yang dibagikan Profil, karena kebijakan default `AWSRAMPermissionRoute53ProfileAllowAssociation` tidak menyertakannya.

Izin untuk konsumen

Izin default untuk konsumen Profil bersama adalah hanya-baca. Dengan izin hanya-baca, mereka dapat melihat sumber daya terkait dan mengaitkannya VPCs, tetapi tidak dapat mengelola asosiasi sumber daya.

Pemilik juga dapat membuat izin terkelola pelanggan di AWS RAM konsol. Untuk informasi selengkapnya, lihat [Membuat dan menggunakan izin terkelola pelanggan](#) di Panduan AWS RAM Pengguna.

Tagihan dan pengukuran

Profil Route 53 ditagih berdasarkan jumlah asosiasi VPC. Pemilik Profil bertanggung jawab atas tagihan untuk asosiasi VPC oleh pelanggan.

Kuota contoh

Pemilik Profil dan konsumen berbagi kuota yang sama, kecuali jumlah Profil Route 53 per akun di suatu Wilayah. Untuk informasi selengkapnya, lihat [Kuota pada Profil Route 53](#)

Apa itu Amazon Route 53 di Outposts?

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layanan APIs, dan alat ke tempat pelanggan. Hal ini memungkinkan pelanggan untuk menjalankan AWS layanan dengan beban kerja lokal dengan menggunakan antarmuka pemrograman yang sama seperti di Wilayah AWS. Untuk informasi lebih lanjut, lihat [Apa itu AWS Outposts?](#) dalam AWS Outposts User Guide.

Route 53 di Outposts menawarkan dua kemampuan:

- Resolver VPC yang menyimpan semua kueri DNS yang berasal dari file. AWS Outposts
- Konektivitas hibrid antara Outpost dan resolver DNS lokal saat Anda menerapkan titik akhir masuk dan keluar.

Untuk informasi selengkapnya, lihat [Apa itu Route 53 VPC Resolver?](#).

Selain itu, Route 53 di Outposts mengurangi latensi jaringan dengan memungkinkan kueri diselesaikan dalam Outpost alih-alih melakukan perjalanan pulang pergi ke yang terdekat. Wilayah AWS

- Resolver VPC yang menyimpan semua kueri DNS yang berasal dari file. AWS Outposts
- Konektivitas hibrid antara Outpost dan resolver DNS lokal saat Anda menerapkan titik akhir masuk dan keluar.

Untuk informasi selengkapnya, lihat [Apa itu Route 53 VPC Resolver?](#).

Selain itu, Route 53 di Outposts mengurangi latensi jaringan dengan memungkinkan kueri diselesaikan dalam Outpost alih-alih melakukan perjalanan pulang pergi ke yang terdekat. Wilayah AWS

Note

Jika Anda memiliki versi AWS Outposts rak yang tidak kompatibel dengan Route 53 di Outposts, tim AWS akan memberi tahu dan akan menghubungi Anda untuk membantu Anda meningkatkan. AWS Outposts

Gambaran umum arsitektur

Route 53 di Outposts mengimplementasikan arsitektur DNS terdistribusi:

- Catatan DNS dan zona yang dihosting tetap dikelola di Amazon Route 53 di Wilayah AWS
- Fungsionalitas penyelesai meluas ke AWS Outposts rak Anda untuk pemrosesan kueri lokal

Desain ini mengoptimalkan kinerja dan ketersediaan kueri sambil mempertahankan manajemen catatan DNS terpusat. Catatan DNS terus disimpan di AWS Wilayah, bukan secara lokal di rak. AWS Outposts

Amazon Route 53 pada fitur Outposts

Tabel berikut menjelaskan bagaimana fitur Route 53 di Outposts dibandingkan dengan fitur Amazon Route 53.

Route 53 di Outposts dibandingkan dengan Route 53

Fitur	Ketersediaan di Route 53 di Outposts
VPC Resolver	Ya. VPC Resolver memelihara cache lokal catatan untuk aplikasi yang dihosting di rak Outpost, VPC yang diintip di, dan nama host yang dapat diakses publik. Wilayah AWS
Pemeriksaan kondisi	Tidak. Pemeriksaan Kesehatan dihitung dan dilaporkan dari Wilayah AWS. Jika Outpost terputus dari cloud, titik akhir gagal terbuka dan tidak dapat gagal ke cadangan.
Titik akhir penyelesai	Ya. Titik akhir Resolver di rak Outpost memungkinkan kueri DNS diteruskan dan diterima dari server DNS lokal. Hanya tipe IPv4 titik akhir yang tersedia untuk titik akhir.
Penyelesai DNS Firewall	Tidak tersedia.
Arus lalu lintas	Tidak tersedia.

Perilaku VPC Resolver saat AWS Outposts terputus dari VPC

Jika AWS Outposts terputus dari Wilayah AWS, Resolver di Outpost berperilaku sebagai berikut:

- Perubahan bidang kontrol tidak tersedia.
- Pemeriksaan kesehatan dan kemampuan failover DNS tidak tersedia.
- Kueri DNS untuk sumber daya yang di-host secara lokal di Outposts diselesaikan tetapi dalam beberapa kasus responsnya mungkin basi jika alamat IP untuk sumber daya diperbarui saat Outpost dalam keadaan terputus.
- Kueri DNS untuk sumber daya yang dihosting di VPC In-region dapat diselesaikan. Namun, sumber daya tidak akan dapat diakses sampai koneksi Outpost ke Wilayah AWS dipulihkan.
- Kueri DNS untuk sumber daya DNS publik dapat diselesaikan jika tersedia di cache VPC Resolver di Outpost.

Memulai dengan VPC Resolver aktif AWS Outposts

Setelah Anda memesan AWS Outposts rak Anda dan mereka telah dikirim, seperti yang dijelaskan di sini: [Buat AWS Outposts](#) dalam AWS Outposts panduan, Anda dapat mengatur Resolver di Outpost.

Important

Resolver di Outpost hanya dapat dibuat oleh AWS akun yang memiliki rak. AWS Outposts
Jika AWS Outposts rak dibagikan dengan akun lain, akun tersebut tidak dapat membuat Resolver di Outpost di rak bersama.

Anda juga dapat menggunakan APIs untuk mengelola Route 53 di Outposts. Untuk informasi selengkapnya, lihat [Resolver tentang tindakan Outpost](#).

Important

Diperlukan waktu hingga 30-150 menit untuk membuat cache VPC Resolver pada file. AWS Outposts

Setelah AWS Outposts rak dikirimkan, Anda dapat memilih Route 53 di Outposts.

Untuk mengkonfigurasi Resolver di Outpost

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pada halaman Resolver on Outpost, pilih Create VPC Resolver.
5. Pada halaman Create VPC Resolver:
 - Di bawah AWS Outposts pilih yang AWS Outposts Anda inginkan untuk membuat Resolver VPC aktif.
 - Ketik nama untuk Resolver VPC di kotak teks nama VPC Resolver.
 - Setelah jenis instans yang Direkomendasikan untuk VPC Resolver terisi dengan instans Amazon EC2 , pilih salah satu.

Untuk informasi selengkapnya tentang jenis instance, lihat [Kuota pada Resolver di Outpost](#).

- Untuk Jumlah instans, pilih jumlah instans antarmuka elastis untuk VPC Resolver. Nilai defaultnya adalah 4.

Jika Anda AWS Outposts tidak memiliki tipe instans yang mendukung Resolver VPC, Anda tidak akan dapat membuat Resolver VPC.

6. Pilih Buat Resolver VPC.

Anda dapat memantau pembuatan Resolver VPC di halaman Resolver on Outpost.

Membuat titik akhir masuk

Setelah membuat Resolver di Outpost, Anda dapat menambahkan titik akhir masuk dan keluar untuk menyelesaikan kueri DNS ke dan dari jaringan lokal Anda.

Untuk mengonfigurasi titik akhir masuk untuk Resolver di Outpost

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.

4. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasional dan pilih Lihat detail.
5. Pada tabel Inbound endpoints, pilih Create inbound endpoint.
6. Pada halaman Create inbound endpoint, masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat membuat atau mengedit titik akhir masuk di Outpost](#).
7. Pilih Buat titik akhir.

Nilai yang Anda tentukan saat membuat atau mengedit titik akhir masuk di Outpost

Saat Anda membuat atau mengedit titik akhir masuk, tentukan nilai berikut:

outpost-id

Jika Anda membuat titik akhir untuk Resolver VPC di VPC, AWS Outposts ini adalah ID. AWS Outposts

Nama titik akhir

Nama ramah yang memudahkan Anda menemukan titik akhir masuk di dasbor.

VPC dalam Wilayah region-name

Semua kueri DNS masuk dari jaringan Anda melewati VPC ini dalam perjalanan ke VPC Resolver.

Grup keamanan untuk titik akhir ini

ID dari satu atau beberapa grup keamanan yang ingin Anda gunakan untuk mengontrol akses ke titik akhir masuk ini. Grup keamanan yang Anda tentukan harus menyertakan satu atau lebih aturan masuk. Aturan masuk harus mengizinkan akses TCP dan UDP di port 53. Anda tidak dapat mengubah nilai ini setelah Anda membuat titik akhir.

Untuk informasi selengkapnya, lihat [Grup keamanan untuk VPC Anda](#) di Panduan pengguna Amazon VPC.

Alamat IP

Alamat IP yang ingin Anda tetapkan ke titik akhir masuk. Kami mengharuskan Anda untuk menentukan minimal dua alamat IP untuk redundansi. Perhatikan hal-hal berikut:

Alamat IP dan antarmuka jaringan elastis Amazon VPC

Untuk setiap kombinasi Availability Zone, Subnet, dan alamat IP yang Anda tentukan, VPC Resolver membuat antarmuka elastis network Amazon VPC. Untuk jumlah maksimum kueri DNS saat ini per detik per alamat IP di titik akhir, lihat [Kuota pada Route 53 VPC Resolver](#). Untuk informasi tentang harga untuk setiap elastic network interface, lihat Amazon Route 53 di [halaman harga Amazon Route 53](#).

Note

Titik akhir Resolver memiliki alamat IP pribadi. Alamat IP ini tidak akan berubah selama masa hidup titik akhir.

Untuk setiap alamat IP, tentukan nilai berikut. Setiap alamat IP harus berada dalam Availability Zone di VPC yang Anda tentukan di VPC dalam Wilayah region-name.

Zona Ketersediaan

Availability Zone yang akan dilewati kueri DNS dalam perjalanan ke VPC Anda. Availability Zone yang Anda tentukan harus dikonfigurasi dengan subnet.

Subnet

Subnet yang berisi alamat IP tujuan penerusan kueri DNS. Subnet harus memiliki alamat IP yang tersedia.

Tentukan subnet untuk IPv4 alamat. IPv6 tidak didukung.

Alamat IP

Satu alamat IP tujuan penerusan kueri DNS.

Pilih apakah Anda ingin VPC Resolver memilih alamat IP untuk Anda dari antara alamat IP yang tersedia di subnet yang ditentukan, atau Anda ingin menentukan alamat IP sendiri.

Jika Anda memilih untuk menentukan alamat IP sendiri, masukkan IPv4 alamat. IPv6 tidak didukung.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Ini adalah tag yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda; Anda dapat menggunakan tag untuk tujuan lain juga. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Menggunakan tanda alokasi biaya](#) dalam Panduan Pengguna AWS Billing .

Membuat titik akhir keluar

Setelah memilih dan mengonfigurasi Resolver VPC, Anda juga dapat menambahkan titik akhir masuk dan keluar untuk menyelesaikan kueri DNS ke jaringan lokal.

Note

Saat Anda mengonfigurasi titik akhir keluar, VPC Resolver menyimpan respons DNS dalam cache sehingga kueri masih dapat diselesaikan jika Pos Luar Anda terputus dari Wilayah. Mempertahankan cache ini dapat meningkatkan permintaan DNS ke resolver lokal Anda.

Untuk mengonfigurasi titik akhir keluar untuk Resolver di Outpost

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih tanda centang di sebelah Resolver VPC yang dalam keadaan operasional dan pilih Lihat detail.
5. Pada tabel titik akhir Outbound, pilih Create outbound endpoint.
6. Pada halaman Create outbound endpoint, masukkan nilai yang berlaku. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat Anda membuat atau mengedit titik akhir keluar dalam AWS Outposts](#).
7. Pilih Buat titik akhir.

Nilai yang Anda tentukan saat Anda membuat atau mengedit titik akhir keluar dalam AWS Outposts

Saat Anda membuat atau mengedit titik akhir keluar, tentukan nilai berikut:

outpost-id

Jika Anda membuat titik akhir untuk Resolver VPC di VPC, AWS Outposts ini adalah ID. AWS Outposts

Nama titik akhir

Nama ramah yang memudahkan Anda menemukan titik akhir keluar di dasbor.

VPC dalam Wilayah region-name

Semua kueri DNS keluar dari VPC Anda melewati VPC ini dalam perjalanan ke jaringan Anda.

Grup keamanan untuk titik akhir ini

ID salah satu atau beberapa grup keamanan yang ingin Anda gunakan untuk mengendalikan akses ke VPC ini. Grup keamanan yang Anda tentukan harus menyertakan satu atau lebih aturan keluar. Aturan keluar harus mengizinkan akses TCP dan UDP di port yang Anda gunakan untuk kueri DNS di jaringan. Anda tidak dapat mengubah nilai ini setelah Anda membuat titik akhir.

Untuk informasi selengkapnya, lihat [Grup keamanan untuk VPC Anda](#) di Panduan pengguna Amazon VPC.

Alamat IP

Alamat IP yang ingin Anda tetapkan ke titik akhir keluar. Kami mengharuskan Anda untuk menentukan minimal dua alamat IP untuk redundansi. Perhatikan hal-hal berikut:

Alamat IP dan antarmuka jaringan elastis Amazon VPC

Untuk setiap kombinasi Availability Zone, Subnet, dan alamat IP yang Anda tentukan, VPC Resolver membuat antarmuka elastis network Amazon VPC. Untuk jumlah maksimum kueri DNS saat ini per detik per alamat IP di titik akhir, lihat [Kuota pada Route 53 VPC Resolver](#). Untuk informasi tentang harga untuk setiap elastic network interface, lihat "Amazon Route 53" di halaman [harga Amazon Route 53](#).

Note

Titik akhir Resolver memiliki alamat IP pribadi. Alamat IP ini tidak akan berubah selama masa hidup titik akhir.

Untuk setiap alamat IP, tentukan nilai berikut. Setiap alamat IP harus berada dalam Availability Zone di VPC yang Anda tentukan di VPC dalam Wilayah region-name.

Zona Ketersediaan

Availability Zone yang ingin Anda lewati kueri DNS dalam perjalanan dari VPC Anda. Availability Zone yang Anda tentukan harus dikonfigurasi dengan subnet.

Subnet

Subnet yang berisi alamat IP yang ingin Anda teruskan kueri DNS. Subnet harus memiliki alamat IP yang tersedia.

Tentukan subnet untuk IPv4 alamat. IPv6 tidak didukung.

Alamat IP

Alamat IP yang ingin Anda tetapkan ke titik akhir keluar.

Pilih apakah Anda ingin VPC Resolver memilih alamat IP untuk Anda dari antara alamat IP yang tersedia di subnet yang ditentukan, atau Anda ingin menentukan alamat IP sendiri.

Jika Anda memilih untuk menentukan alamat IP sendiri, masukkan IPv4 alamat. IPv6 tidak didukung.

Tag

Tentukan satu atau lebih kunci dan nilai yang sesuai. Misalnya, Anda dapat menentukan Pusat biaya untuk Kunci dan menentukan 456 untuk Nilai.

Ini adalah tag yang AWS Billing and Cost Management menyediakan untuk mengatur AWS tagihan Anda; Anda juga dapat menggunakan tag untuk tujuan lain. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Menggunakan tanda alokasi biaya](#) dalam Panduan Pengguna AWS Billing .

Membuat aturan penerusan untuk titik akhir keluar

Anda juga dapat membuat aturan penerusan untuk titik akhir keluar. Untuk informasi selengkapnya, lihat [Untuk membuat aturan penerusan dan mengaitkan aturan dengan satu atau lebih VPCs](#)

Mengelola Resolver di Outpost

Untuk mengelola Resolver di Outpost, lakukan prosedur yang berlaku.

Topik

- [Mengedit Resolver di Outpost](#)
- [Melihat Resolver pada status Outpost](#)
- [Menghapus Resolver di Outpost](#)

Mengedit Resolver di Outpost

Untuk mengedit Resolver di Outpost, lakukan prosedur berikut.

Untuk mengedit Resolver di Outpost

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih tanda centang di sebelah Resolver VPC yang dalam keadaan operasional dan pilih Edit.
5. Anda dapat mengedit informasi berikut:
 - Nama VPC Resolver
 - Jenis instance
 - Jumlah contoh
6. Setelah selesai mengedit, pilih Simpan perubahan.

Melihat Resolver pada status Outpost

Untuk melihat status Resolver di Outpost, lakukan prosedur berikut.

Cara melihat status titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih tanda centang di sebelah Resolver VPC yang dalam keadaan operasional dan pilih Lihat detail.
5. Kolom Status di halaman Resolver on Outpost, berisi salah satu nilai berikut:

Membuat

Resolver on Outpost sedang dalam proses pembuatan.

Operasional

Resolver di Outpost dikonfigurasi dengan benar.

Memperbarui

Resolver di Outpost memperbarui jenis instance.

Diperlukan tindakan

Resolver VPC ini tidak sehat dan tidak dapat dipulihkan secara otomatis. Untuk mengatasi masalah ini, kami sarankan Anda memastikan instans AWS Outposts dapat mendukung Resolver di Outpost.

Menghapus

Resolver di Outpost sedang dalam proses dihapus.

Penciptaan yang gagal

Penciptaan Resolver di Outpost gagal.

Penghapusan gagal

Penghapusan Resolver di Outpost gagal. Untuk memperbaiki masalah ini, coba lagi dalam beberapa menit.

Menghapus Resolver di Outpost

Note

Sebelum Anda dapat menghapus Resolver di Outpost, Anda harus terlebih dahulu menghapus titik akhir yang terkait dengannya.

Untuk menghapus Resolver di Outpost, lakukan prosedur berikut.

Untuk menghapus Resolver di Outpost

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih kotak centang di sebelah Resolver VPC yang dalam keadaan operasional dan pilih Hapus.
5. Dalam Hapus Resolver VPC kotak dialog, masukkan **delete** di kotak teks, dan pilih Hapus.

Mengelola titik akhir masuk pada Resolver di Outpost

Untuk mengelola titik akhir masuk pada Resolver di Outpost, lakukan prosedur yang berlaku.

Topik

- [Melihat dan mengedit titik akhir masuk](#)
- [Melihat status titik akhir masuk](#)
- [Menghapus titik akhir masuk](#)

Melihat dan mengedit titik akhir masuk

Untuk melihat dan mengedit pengaturan titik akhir masuk, lakukan prosedur berikut.

Cara melihat dan mengedit pengaturan untuk titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasional dan pilih Lihat detail.
5. Dalam daftar titik akhir Inbound, pilih opsi untuk titik akhir yang ingin Anda lihat setelan atau ingin edit.
6. Pilih Tampilkan detail atau Edit.

Untuk informasi tentang nilai titik akhir masuk, lihat [Nilai yang Anda tentukan saat Anda membuat atau mengedit titik akhir keluar dalam AWS Outposts](#).

7. Jika Anda memilih Edit, masukkan nilai yang berlaku, dan pilih Simpan.

Melihat status titik akhir masuk

Untuk melihat status titik akhir masuk, lakukan prosedur berikut.

Cara melihat status titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasi dan pilih Lihat detail.
5. Kolom Status dari daftar titik akhir masuk berisi salah satu nilai berikut:

Membuat

VPC Resolver membuat dan mengonfigurasi satu atau lebih antarmuka jaringan VPC Amazon untuk titik akhir ini.

Operasional

Antarmuka jaringan VPC Amazon untuk titik akhir ini dikonfigurasi dengan benar dan dapat meneruskan kueri DNS masuk atau keluar antara jaringan Anda dan VPC Resolver.

Memperbarui

Resolver mengaitkan atau memisahkan satu atau lebih antarmuka jaringan dengan titik akhir ini.

Memulihkan otomatis

VPC Resolver mencoba memulihkan satu atau lebih antarmuka jaringan yang terkait dengan titik akhir ini. Selama proses pemulihan, titik akhir berfungsi dengan kapasitas terbatas karena batas jumlah kueri DNS per alamat IP (per antarmuka jaringan). Untuk batas saat ini, lihat [Kuota pada Route 53 VPC Resolver](#).

Diperlukan tindakan

Titik akhir ini tidak sehat, dan VPC Resolver tidak dapat memulihkannya secara otomatis.

Untuk mengatasi masalah, kami sarankan Anda memeriksa setiap alamat IP yang dikaitkan

dengan titik akhir. Untuk setiap alamat IP yang tidak tersedia, tambahkan alamat IP lain, lalu hapus alamat IP yang tidak tersedia. Endpoint harus selalu menyertakan setidaknya dua alamat IP. Status Diperlukan tindakan dapat memiliki berbagai penyebab. Berikut adalah dua penyebab umum:

- Satu atau lebih antarmuka jaringan yang terkait dengan titik akhir dihapus menggunakan Amazon VPC.
- Antarmuka jaringan tidak dapat dibuat karena alasan tertentu yang berada di luar kendali VPC Resolver.

Menghapus

Resolver menghapus titik akhir ini dan antarmuka jaringan yang terkait.

Menghapus titik akhir masuk

Untuk menghapus titik akhir masuk, lakukan prosedur berikut.

Important

Jika Anda menghapus titik akhir masuk, kueri DNS dari jaringan Anda tidak lagi diteruskan ke VPC Resolver di VPC yang Anda tentukan di titik akhir.

Cara menghapus titik akhir masuk

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasi dan pilih Lihat detail.
5. Pilih kotak centang di sebelah titik akhir yang ingin Anda hapus.
6. Pilih Hapus.
7. Untuk mengonfirmasi bahwa Anda ingin menghapus titik akhir, masukkan nama titik akhir dan pilih Kirim.

Mengelola titik akhir keluar pada Resolver di Outpost

Untuk mengelola titik akhir keluar pada Resolver di Outpost, lakukan prosedur yang berlaku.

Topik

- [Melihat dan mengedit titik akhir keluar](#)
- [Melihat status titik akhir keluar](#)
- [Menghapus titik akhir keluar](#)

Melihat dan mengedit titik akhir keluar

Untuk melihat dan mengedit pengaturan titik akhir keluar, lakukan prosedur berikut.

Cara melihat dan mengedit pengaturan untuk titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasi dan pilih Lihat detail.
5. Dalam daftar Titik akhir keluar, pilih kotak centang di sebelah titik akhir yang ingin Anda lihat setelan atau ingin edit.
6. Pilih Tampilkan detail atau Edit.

Untuk informasi tentang nilai titik akhir keluar, lihat [Nilai yang Anda tentukan saat Anda membuat atau mengedit titik akhir keluar dalam AWS Outposts](#).

7. Jika Anda memilih Edit, masukkan nilai yang berlaku, lalu pilih Simpan.

Melihat status titik akhir keluar

Untuk melihat status titik akhir keluar, lakukan prosedur berikut.

Cara melihat status titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pada bilah navigasi, pilih Wilayah tempat Anda AWS Outposts berada.
4. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasi dan pilih Lihat detail.
5. Dalam daftar titik akhir Outbound, kolom Status berisi salah satu nilai berikut:

Membuat

VPC Resolver membuat dan mengonfigurasi satu atau lebih antarmuka jaringan VPC Amazon untuk titik akhir ini.

Operasional

Antarmuka jaringan VPC Amazon untuk titik akhir ini dikonfigurasi dengan benar dan dapat meneruskan kueri DNS masuk atau keluar antara jaringan Anda dan VPC Resolver.

Memperbarui

Resolver mengaitkan atau memisahkan satu atau lebih antarmuka jaringan dengan titik akhir ini.

Memulihkan otomatis

VPC Resolver mencoba memulihkan satu atau lebih antarmuka jaringan yang terkait dengan titik akhir ini. Selama proses pemulihan, titik akhir berfungsi dengan kapasitas terbatas karena batas jumlah kueri DNS per alamat IP (per antarmuka jaringan). Untuk batas saat ini, lihat [Kuota pada Route 53 VPC Resolver](#).

Diperlukan tindakan

Titik akhir ini tidak sehat, dan VPC Resolver tidak dapat memulihkannya secara otomatis. Untuk mengatasi masalah, kami sarankan Anda memeriksa setiap alamat IP yang dikaitkan dengan titik akhir. Untuk setiap alamat IP yang tidak tersedia, tambahkan alamat IP lain, lalu hapus alamat IP yang tidak tersedia. (Titik akhir harus selalu menyertakan setidaknya dua alamat IP.) Status Diperlukan tindakan dapat memiliki berbagai penyebab. Berikut adalah dua penyebab umum:

- Satu atau lebih antarmuka jaringan yang terkait dengan titik akhir dihapus menggunakan Amazon VPC.
- Antarmuka jaringan tidak dapat dibuat karena alasan tertentu yang berada di luar kendali VPC Resolver.

Menghapus

Resolver menghapus titik akhir ini dan antarmuka jaringan yang terkait.

Menghapus titik akhir keluar

Sebelum Anda dapat menghapus titik akhir, Anda harus terlebih dahulu menghapus aturan apa pun yang terkait dengan VPC.

Untuk menghapus titik akhir keluar, lakukan prosedur berikut.

Important

Jika Anda menghapus titik akhir keluar, VPC Resolver berhenti meneruskan kueri DNS dari VPC ke jaringan Anda untuk aturan yang menentukan titik akhir keluar yang dihapus.

Cara menghapus titik akhir keluar

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi kiri, perluas Resolver, lalu arahkan ke Outposts.
3. Pilih kotak centang di sebelah Resolver VPC yang dalam status operasi dan pilih Lihat detail.
4. Dalam daftar titik akhir Outbound pilih opsi untuk titik akhir yang ingin Anda hapus.
5. Pilih Hapus.
6. Untuk mengonfirmasi bahwa Anda ingin menghapus titik akhir, masukkan nama titik akhir, lalu pilih Kirim.

Apa itu Route 53 Global Resolver?

Route 53 Global Resolver adalah resolver DNS yang dapat dijangkau internet yang menyediakan resolusi DNS yang mudah, aman, dan andal untuk klien resmi di organisasi Anda di lokasi terpencil, kantor cabang, dan lingkungan lokal. Anda dapat menyelesaikan kueri untuk domain yang dihosting di Amazon Route 53 zona yang dihosting pribadi atau domain publik di internet, sambil mempertahankan ketersediaan tinggi melalui arsitektur anycast global. Route 53 Global Resolver membantu Anda melindungi klien Anda dari serangan eksfiltrasi data berbasis DNS, dengan memfilter kueri ke domain yang berpotensi berbahaya.

Route 53 Global Resolver menggunakan alamat IP anycast yang secara otomatis merutekan kueri DNS ke AWS Wilayah terdekat dengan lokasi kueri sumber Anda untuk latensi dan ketersediaan yang optimal. Anda dapat memilih wilayah tempat resolver global Anda harus menyediakan resolusi DNS untuk klien resmi Anda, mengonfigurasi tampilan berbeda untuk klien untuk resolusi domain pribadi dan publik, memfilter domain berbahaya, dan memantau aktivitas DNS di seluruh organisasi Anda.

Topik

- [Mengapa Route 53 Global Resolver?](#)
- [Konsep dan komponen kunci untuk Route 53 Global Resolver](#)
- [Cara kerja Route 53 Global Resolver](#)
- [Keamanan DNS dan kasus penggunaan cakrawala terpisah untuk Route 53 Global Resolver](#)
- [AWS layanan yang terintegrasi dengan Route 53 Global Resolver untuk meningkatkan keamanan DNS](#)
- [Cara mengakses dan mengelola Route 53 Global Resolver melalui antarmuka AWS](#)
- [Didukung Wilayah AWS](#)
- [Menyiapkan akses akun untuk Route 53 Global Resolver](#)
- [Tutorial: Buat Resolver Global Route 53 pertama Anda](#)
- [Mengelola tampilan DNS dengan Route 53 Global Resolver](#)
- [Mengelola kontrol akses dengan sumber akses dan token di Route 53 Global Resolver](#)
- [Mengamankan DNS untuk klien dengan Route 53 Global Resolver](#)
- [Mengkonfigurasi asosiasi zona host pribadi dengan Route 53 Global Resolver](#)
- [Memantau aktivitas dan kinerja DNS dengan Route 53 Global Resolver](#)
- [Memecahkan masalah DNS dengan Route 53 Global Resolver](#)

- [Kuota untuk Route 53 Global Resolver](#)

Mengapa Route 53 Global Resolver?

Route 53 Global Resolver menyediakan keamanan dan pemfilteran DNS terpusat untuk klien jarak jauh dan hibrida serta beban kerja di beberapa lokasi. Terlepas dari lokasi beban kerja, aplikasi, atau pengguna Anda, Route 53 Global Resolver memastikan perlindungan DNS yang konsisten tanpa memerlukan infrastruktur lokal yang kompleks.

Manfaat utama untuk lingkungan jarak jauh dan hibrida:

- Manajemen yang disederhanakan - Konfigurasikan resolusi domain pribadi dan publik menggunakan solusi tunggal alih-alih mengelola beberapa server DNS lokal
- Keamanan DNS terpadu - Menerapkan kebijakan pemfilteran yang konsisten di semua klien jarak jauh dan beban kerja hybrid
- Perlindungan yang dapat diskalakan - Secara otomatis menskalakan untuk menangani kueri DNS dari tenaga kerja jarak jauh dan beban kerja cloud yang terus bertambah
- Mengurangi infrastruktur - Meminimalkan kebutuhan akan peralatan keamanan DNS di setiap lokasi terpencil

Untuk memulai, lihat:

- [the section called “Konsep dan terminologi”](#)- Konsep inti untuk penyebaran keamanan DNS
- [the section called “Cara kerjanya”](#)- Bagaimana Route 53 Global Resolver melindungi lingkungan jarak jauh dan hibrida
- [the section called “Tutorial: Buat Resolver Global Route 53 pertama Anda”](#)- Tutorial untuk pengaturan penyaringan DNS pertama Anda

Konsep dan komponen kunci untuk Route 53 Global Resolver

Route 53 Global Resolver menggunakan beberapa komponen kunci yang bekerja sama untuk menyediakan resolusi DNS split-traffic, ketersediaan tinggi melalui arsitektur anycast global, dan keamanan DNS komprehensif untuk organisasi Anda. Memahami konsep Route 53 Global Resolver ini membantu Anda merancang dan menerapkan solusi yang memungkinkan akses tanpa batas ke sumber daya swasta dan publik, memastikan kelangsungan layanan di berbagai Wilayah, dan melindungi dari ancaman berbasis DNS.

DNS resolver untuk klien di lokasi lokal dan terpencil

Untuk menerapkan Route 53 Global Resolver untuk beban kerja terdistribusi, lokasi pelanggan, dan pengguna, konfigurasi komponen utama ini:

Penyelesai global

Instans layanan utama yang menyediakan resolusi dan pemfilteran DNS untuk organisasi Anda di beberapa AWS Wilayah. Penyelesai global Anda menggunakan teknologi anycast untuk secara otomatis merutekan kueri DNS ke Wilayah terdekat yang tersedia, memastikan waktu respons yang cepat untuk semua klien terlepas dari lokasi mereka.

Alamat IP anycast

Dua IPv6 alamat unik IPv4 atau yang ditetapkan ke resolver global yang Anda konfigurasi pada perangkat klien dan peralatan jaringan. Alamat IP anycast ini sama secara global, yang menyederhanakan konfigurasi DNS di semua lokasi Anda. Pengalamatan IP Anycast memungkinkan perutean otomatis permintaan DNS ke resolver global terdekat, mengoptimalkan waktu respons dan meningkatkan keandalan layanan.

Tampilan DNS

Templat konfigurasi yang memungkinkan Anda menerapkan kebijakan DNS yang berbeda ke grup klien yang berbeda di jaringan Anda. Gunakan tampilan DNS untuk menerapkan DNS split-horizon — Misalnya, terapkan pemfilteran ketat dan otentikasi token untuk lokasi terpencil, saat menggunakan akses berbasis IP dan kebijakan keamanan yang berbeda untuk kantor cabang.

Autentikasi klien DNS

Pilih metode otentikasi yang paling sesuai untuk penerapan Anda:

Otentikasi berbasis token

Amankan koneksi DNS menggunakan token terenkripsi untuk DNS-over-HTTPS (DoH) dan DNS-over-TLS (DoT). Anda dapat menghasilkan token akses unik untuk klien individu atau grup perangkat, menetapkan periode kedaluwarsa, dan mencabut token sesuai kebutuhan.

Akses otentikasi berbasis sumber

Kontrol akses menggunakan alamat IP dan daftar izin rentang CIDR. Anda dapat mengonfigurasi alamat IP publik kantor cabang atau rentang jaringan, lalu menentukan protokol DNS (DNS-over-

port-53, DoT, atau DoH) yang dapat digunakan setiap lokasi berdasarkan persyaratan keamanan Anda.

Pemilihan protokol DNS

Pilih protokol DNS yang sesuai berdasarkan kebutuhan keamanan dan kompatibilitas Anda:

- DNS-over-port-53 (Do53) - Gunakan untuk kompatibilitas maksimum dengan infrastruktur jaringan yang ada
- DNS-over-TLS (DoT) - Gunakan saat Anda membutuhkan DNS terenkripsi dengan pemisahan port khusus untuk pemantauan jaringan
- DNS-over-HTTPS (DoH) - Gunakan saat Anda perlu melewati batasan jaringan, karena lalu lintas muncul sebagai HTTPS biasa

Resolusi DNS lalu lintas terpisah

Route 53 Global Resolver memungkinkan organisasi menyelesaikan domain pribadi dan publik dengan mulus dari lokasi mana pun, menghilangkan kebutuhan akan konfigurasi VPN yang kompleks atau pengaturan DNS khusus Wilayah.

Resolusi DNS hibrida

Resolusi DNS Hybrid memungkinkan Route 53 Global Resolver untuk secara bersamaan menyelesaikan kueri dari pengguna dan aplikasi lokal ke aplikasi pribadi. AWS

Akses zona pribadi global

Akses zona pribadi global memperluas jangkauan zona host pribadi Amazon Route 53 di luar batas VPC. Klien resmi di mana saja di internet dapat menyelesaikan nama domain pribadi, memungkinkan tim terdistribusi untuk mengakses sumber daya internal tanpa persyaratan konektivitas jaringan tradisional.

Failover mulus

Failover yang mulus memastikan akses berkelanjutan ke sumber daya swasta dan publik bahkan ketika AWS Wilayah individu menjadi tidak tersedia. Arsitektur anycast secara otomatis merutekan kueri ke wilayah sehat sambil mempertahankan perilaku resolusi yang konsisten.

Ketersediaan tinggi dan kehadiran global

Route 53 Global Resolver menyediakan ketersediaan tingkat perusahaan melalui arsitektur terdistribusi dan kemampuan failover otomatis.

Penyebaran multi-wilayah

Penerapan multi-wilayah mendistribusikan instans Route 53 Global Resolver di setidaknya 2 AWS Wilayah untuk memastikan ketersediaan tinggi dan memungkinkan failover selama pemadaman layanan. Anda dapat memilih Wilayah tertentu berdasarkan persyaratan geografis dan kebutuhan kepatuhan Anda.

Optimalisasi geografis otomatis

Optimasi geografis otomatis merutekan kueri DNS ke AWS Wilayah terdekat yang tersedia berdasarkan topologi dan latensi jaringan. Ini mengurangi waktu respons dan meningkatkan pengalaman pengguna untuk organisasi yang didistribusikan secara global.

Redundansi bawaan

Redundansi bawaan memastikan kontinuitas layanan melalui failover otomatis ke wilayah alternatif ketika wilayah utama menjadi tidak tersedia. Klien terus menggunakan alamat IP anycast yang sama sementara lalu lintas dialihkan secara transparan.

Resolusi dan penerusan DNS

Resolusi zona yang dihosting pribadi

Resolusi zona yang dihosting pribadi memungkinkan Route 53 Global Resolver untuk menyelesaikan kueri DNS untuk zona host pribadi Route 53 di seluruh Wilayah. AWS Ini memungkinkan klien yang berwenang untuk menyelesaikan domain untuk aplikasi dan sumber daya yang dihosting oleh Route 53 dari mana saja di internet.

DNS cakrawala terpisah

DNS split-horizon menyediakan respons DNS yang berbeda berdasarkan klien yang membuat kueri. Route 53 Global Resolver dapat menyelesaikan domain publik di internet sekaligus menyelesaikan domain pribadi, menyediakan akses tanpa batas ke sumber daya publik dan swasta.

Validasi DNSSEC

Validasi DNSSEC memverifikasi keaslian dan integritas respons DNS dari server nama publik untuk domain yang ditandatangani DNSSEC. Validasi ini memastikan respons DNS tidak dirusak selama transmisi, memberikan perlindungan terhadap spoofing DNS dan serangan keracunan cache.

Subnet Klien EDNS (ECS)

EDNS Client Subnet adalah fitur opsional yang meneruskan informasi subnet klien dalam kueri DNS ke server nama otoritatif. Ini memungkinkan respons DNS berbasis geografis yang lebih akurat, berpotensi mengurangi latensi dengan mengarahkan klien ke jaringan atau server pengiriman konten yang lebih dekat. Untuk koneksi DNS-over-TLS (DoT) dan DNS-over-HTTPS (DoH), Anda dapat menggunakan EDNS0 untuk meneruskan informasi alamat IP klien. Ketika ECS diaktifkan pada Global Resolver, layanan secara otomatis menyuntikkan IP klien jika tidak disediakan dalam kueri.

Pemfilteran DNS dan daftar domain

Route 53 Global Resolver menyediakan pemfilteran berbasis domain menggunakan daftar domain yang dikelola oleh AWS untuk memblokir atau mengizinkan domain tertentu.

Aturan penyaringan DNS

Aturan pemfilteran DNS menentukan cara Route 53 Global Resolver menangani kueri DNS berdasarkan kriteria pencocokan domain. Aturan dievaluasi dalam urutan prioritas dan dapat menentukan tindakan (ALLOW, BLOCK, atau ALERT) untuk kueri ke domain atau kategori domain tertentu.

Daftar domain

Daftar domain adalah kumpulan domain yang digunakan dalam aturan pemfilteran. Mereka bisa:

- Daftar domain khusus - Koleksi domain yang Anda buat dan pelihara
- AWS daftar domain terkelola - Daftar ancaman yang telah dikonfigurasi sebelumnya dan kategori konten yang dikelola oleh AWS yang memanfaatkan intelijen ancaman untuk mengidentifikasi domain berbahaya. Daftar ancaman yang tersedia meliputi:
 - Domain malware - Domain yang dikenal untuk meng-host atau mendistribusikan malware
 - Perintah dan kontrol botnet - Domain yang digunakan oleh botnet untuk komunikasi perintah dan kontrol

- Spam - Domain yang terkait dengan spam dan kampanye email yang tidak diinginkan
- Phishing - Domain yang digunakan dalam serangan phishing untuk mencuri kredensial dan informasi pribadi
- Daftar GuardDuty ancaman Amazon - Domain diidentifikasi oleh intelijen GuardDuty ancaman

Kategori konten yang tersedia termasuk media sosial, perjudian, dan kategori lain yang membantu organisasi mengontrol akses ke jenis konten tertentu.

Spesifikasi domain individual dalam daftar terkelola tidak dapat dilihat atau diedit untuk melindungi kekayaan intelektual dan menjaga efektivitas keamanan.

Deteksi ancaman DNS tingkat lanjut

Route 53 Global Resolver menggunakan analisis algoritmik dinamis untuk mendeteksi ancaman DNS tingkat lanjut seperti tunneling DNS dan Algoritma Pembuatan Domain. Tidak seperti daftar domain yang cocok dengan domain buruk yang diketahui, deteksi algoritmik menganalisis pola kueri DNS secara real-time untuk mengidentifikasi perilaku yang mencurigakan.

Deteksi terowongan DNS

Tunneling DNS digunakan oleh penyerang untuk mengekstraksi data dari klien dengan menggunakan terowongan DNS tanpa membuat koneksi jaringan ke klien.

Deteksi Algoritma Pembuatan Domain (DGA)

Domain Generation Algorithms (DGAs) digunakan oleh penyerang untuk membuat sejumlah besar nama domain untuk servernya command-and-control.

Ambang kepercayaan

Setiap algoritma deteksi menghasilkan skor kepercayaan yang menentukan pemicu aturan. Ambang kepercayaan yang lebih tinggi mengurangi positif palsu tetapi mungkin melewatkan serangan canggih. Ambang batas yang lebih rendah meningkatkan sensitivitas deteksi tetapi memerlukan analisis peringatan tambahan untuk menyaring positif palsu.

Batasan tindakan

Aturan perlindungan ancaman tingkat lanjut hanya mendukung ALERT dan BLOCK tindakan. ALLOWTindakan ini tidak didukung karena deteksi algoritmik tidak dapat secara definitif mengklasifikasikan lalu lintas jinak, hanya mengidentifikasi pola yang berpotensi berbahaya.

Pencatatan dan pemantauan

Log kueri

Log kueri memberikan informasi rinci tentang kueri DNS yang diproses oleh Route 53 Global Resolver, termasuk IP sumber, domain kueri, kode respons, tindakan kebijakan yang diambil, dan cap waktu. Log dapat dikirimkan ke Amazon CloudWatch, Amazon Data Firehose, atau Amazon Simple Storage Service untuk analisis dan pelaporan kepatuhan.

Format OCSF

Format Open Cybersecurity Schema Framework (OCSF) adalah format logging standar yang digunakan oleh Route 53 Global Resolver untuk log query DNS. Format ini menyediakan data yang konsisten dan terstruktur yang terintegrasi dengan mudah dengan sistem informasi keamanan dan manajemen peristiwa (SIEM) dan alat keamanan lainnya.

Log tujuan

Tujuan log menentukan di mana log kueri DNS dikirimkan, masing-masing dengan karakteristik yang berbeda:

- Amazon Simple Storage Service - Penyimpanan jangka panjang hemat biaya yang ideal untuk kepatuhan dan analisis batch. Terintegrasi dengan alat analitik seperti Amazon Athena dan Amazon EMR.
- Amazon CloudWatch Logs - Pemantauan dan peringatan waktu nyata dengan integrasi ke CloudWatch alarm dan dasbor Amazon. Mendukung wawasan log untuk kueri ad-hoc.
- Amazon Data Firehose - Streaming real-time ke sistem eksternal dengan kemampuan transformasi data bawaan. Mendukung penskalaan dan buffering otomatis.

Wilayah Observabilitas

Wilayah Observabilitas menentukan tempat log kueri DNS dikirimkan.

Cara kerja Route 53 Global Resolver

Route 53 Global Resolver memungkinkan resolusi DNS split-traffic antara domain publik dan pribadi, menyediakan ketersediaan tinggi melalui dua atau lebih yang Wilayah AWS Anda pilih, dan mengamankan kueri DNS dengan mencegah permintaan dan menerapkan kebijakan pemfilteran DNS. Memahami proses ini membantu Anda memecahkan masalah dan mengoptimalkan penerapan untuk kinerja, ketersediaan, dan keamanan.

Apa yang terjadi ketika klien membuat kueri DNS

Ketika seseorang di lokasi Anda mencoba menanyakan domain, Route 53 Global Resolver memproses permintaan DNS mereka melalui beberapa lapisan keamanan.

Pemrosesan kueri DNS melibatkan langkah-langkah berurutan ini:

1. **Penerimaan kueri** - Perangkat klien mengirim kueri DNS ke alamat IP anycast Route 53 Global Resolver. Perutean anycast secara otomatis mengarahkan kueri ke Wilayah terdekat AWS.
2. **Otentikasi** - Route 53 Global Resolver mengotentikasi klien menggunakan metode otentikasi yang dikonfigurasi (berbasis token untuk DoH/DoT atau Sumber Akses IP untuk semua protokol).
3. **Evaluasi kebijakan** - Layanan mengevaluasi kueri DNS terhadap kebijakan keamanan dan daftar domain yang dikonfigurasi untuk menentukan tindakan yang sesuai (izinkan, blokir, atau peringatan). Untuk kueri yang menargetkan zona host pribadi, Route 53 Global Resolver memeriksa apakah klien diberi wewenang untuk mengakses domain pribadi berdasarkan aturan tampilan DNS yang dikelola oleh administrator Anda sebelum melanjutkan dengan resolusi.
4. **Resolusi** - Untuk kueri yang diizinkan, Route 53 Global Resolver melakukan resolusi DNS menggunakan resolver DNS publik atau resolusi zona host pribadi yang sesuai.
5. **Pengiriman respons** - Layanan mengembalikan respons DNS ke klien dan mencatat detail kueri untuk pemantauan dan analisis.

Arsitektur anycast global

Route 53 Global Resolver menggunakan alamat IP anycast untuk menyediakan ketersediaan global dan perutean geografis otomatis.

Route 53 Global Resolver menggunakan alamat IP anycast untuk menyediakan:

- **Perutean geografis otomatis** - Kueri DNS secara otomatis dirutekan ke Wilayah terdekat AWS untuk kinerja optimal.
- **Redundansi bawaan** - Jika Wilayah menjadi tidak tersedia, lalu lintas secara otomatis gagal ke Wilayah terdekat berikutnya.
- **Alamat IP yang konsisten** - Klien menggunakan alamat IP anycast yang sama terlepas dari lokasi mereka, menyederhanakan konfigurasi.

Pemfilteran dan keamanan DNS

Route 53 Global Resolver menyediakan pemfilteran dan keamanan DNS komprehensif melalui beberapa lapisan. Diagram pemfilteran DNS dan arsitektur keamanan menggambarkan bagaimana kueri diproses melalui autentikasi, evaluasi kebijakan, dan lapisan resolusi.

Route 53 Global Resolver menyediakan keamanan DNS komprehensif melalui:

- Pemfilteran berbasis domain - Blokir atau izinkan kueri berdasarkan nama domain menggunakan daftar domain khusus atau AWS terkelola.
- Integrasi intelijen ancaman - Memanfaatkan intelijen ancaman AWS terkelola untuk secara otomatis memblokir domain berbahaya yang diketahui.
- Deteksi ancaman lanjutan - Mendeteksi dan memblokir upaya tunneling DNS dan pola Algoritma Pembuatan Domain (DGA).
- Pemantauan waktu nyata - Hasilkan peringatan dan log untuk peristiwa keamanan dan pelanggaran kebijakan.

Keamanan DNS dan kasus penggunaan cakrawala terpisah untuk Route 53 Global Resolver

Route 53 Global Resolver membahas tiga tantangan DNS utama untuk organisasi:

Mengaktifkan split-traffic antara resolusi DNS publik dan pribadi

Aktifkan akses global ke zona yang dihosting pribadi (PHZs) di Amazon Route 53 dari lokasi mana pun sekaligus menyelesaikan domain publik di internet. Izinkan lokasi terpencil dan kantor cabang untuk menyelesaikan nama aplikasi internal tanpa konfigurasi VPN yang rumit atau penerusan khusus Wilayah. Terapkan DNS split-horizon untuk memberikan respons DNS yang berbeda berdasarkan klien yang membuat kueri, membantu klien jarak jauh menyelesaikan kueri untuk domain pribadi dan publik.

Mengamankan lalu lintas DNS dari serangan eksfiltrasi DNS

Lindungi lokasi terpencil dan kantor cabang dari serangan eksfiltrasi data berbasis DNS dengan memfilter kueri ke domain berbahaya. Tingkatkan privasi dengan mengenkripsi lalu lintas DNS in-transit menggunakan DNS-over-HTTPS (DoH) dan DNS-over-TLS (DoT) untuk memastikan hanya klien yang berwenang yang dapat mengakses layanan DNS Anda. Terapkan kebijakan

keamanan untuk memblokir ancaman seperti tunneling DNS dan Algoritma Pembuatan Domain (). DGAs Validasi keaslian respons DNS menggunakan DNSSEC (Ekstensi Keamanan Sistem Nama Domain) untuk domain yang ditandatangani DNSSEC untuk melindungi terhadap serangan spoofing DNS dan keracunan cache.

Ketersediaan tinggi dan kehadiran global

Dapatkan ketersediaan tinggi melalui penyebaran global dan pertahankan konfigurasi DNS yang konsisten di seluruh dunia dari satu antarmuka manajemen. Route 53 Global Resolver berjalan melintasi yang Wilayah AWS Anda pilih, menggunakan alamat IP anycast yang secara otomatis merutekan kueri ke Wilayah terdekat yang tersedia untuk kinerja dan keandalan yang optimal. Perusahaan global dapat mengkonfigurasi dan mengelola kebijakan DNS secara terpusat sambil menyediakan klien dengan satu set alamat IP yang bekerja secara global dengan optimasi geografis otomatis. Redundansi bawaan memastikan kontinuitas layanan bahkan jika Wilayah individu menjadi tidak tersedia.

Kemampuan tambahan mendukung kasus penggunaan utama ini:

Menerapkan kebijakan penyaringan dan konten DNS

Mengatur akses internet di beberapa lokasi dengan membuat daftar domain khusus atau menggunakan Daftar Domain AWS Terkelola. Untuk membantu Anda menerapkan kebijakan pemfilteran dan konten sesuai dengan kebutuhan Anda, Daftar Domain Terkelola menyertakan beberapa kategori ancaman DNS yang mencakup beberapa domain. Konfigurasi Sumber Akses menggunakan daftar izin IP atau Token Akses, dan siapkan kebijakan pemfilteran yang berbeda untuk lokasi kantor atau grup klien yang berbeda.

Otentikasi fleksibel untuk skenario penerapan yang berbeda

Pilih metode otentikasi yang paling sesuai untuk penerapan Anda: otentikasi berbasis token atau otentikasi berbasis IP menggunakan daftar izin rentang CIDR sumber.

Mempertahankan visibilitas dan kepatuhan

Pantau aktivitas DNS di seluruh organisasi Anda dengan mengirimkan log ke Amazon CloudWatch, Firehose, atau Amazon Simple Storage Service. Pilih satu Wilayah tujuan untuk penyimpanan log terpusat guna mendukung audit keamanan, persyaratan kepatuhan, dan investigasi ancaman.

AWS layanan yang terintegrasi dengan Route 53 Global Resolver untuk meningkatkan keamanan DNS

Route 53 Global Resolver terintegrasi secara mulus dengan AWS layanan lain untuk memberikan kemampuan keamanan dan manajemen DNS yang komprehensif. Integrasi ini meningkatkan fungsionalitas inti Route 53 Global Resolver dan memungkinkan kasus penggunaan lanjutan:

Amazon Route 53

Route 53 Global Resolver terintegrasi dengan Amazon Route 53 untuk menyelesaikan zona host pribadi secara global. Untuk informasi lebih lanjut, lihat [Panduan Pengembang Amazon Route 53](#).

Amazon CloudWatch

Route 53 Global Resolver dapat mengirimkan log kueri ke Amazon CloudWatch untuk pemantauan dan analisis. Untuk informasi lebih lanjut, lihat [Panduan Pengguna Amazon CloudWatch](#).

Amazon Simple Storage Service

Route 53 Global Resolver dapat menyimpan log kueri di bucket Amazon Simple Storage Service untuk penyimpanan dan analisis jangka panjang. Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon S3](#).

Amazon Data Firehose

Route 53 Global Resolver dapat mengalirkan log kueri ke Amazon Data Firehose untuk pemrosesan waktu nyata. Untuk informasi selengkapnya, lihat [Panduan Pengembang Amazon Data Firehose](#).

Route 53 Resolver DNS Firewall

Route 53 Global Resolver melengkapi Route 53 Resolver DNS Firewall dengan menyediakan kemampuan penyaringan DNS global. Untuk informasi selengkapnya, lihat dokumentasi [Route 53 Resolver DNS Firewall](#).

AWS Global Accelerator

Route 53 Global Resolver bekerja sama AWS Global Accelerator untuk memberikan kinerja jaringan global yang dioptimalkan untuk resolusi DNS. Lihat informasi selengkapnya di [Panduan Developer AWS Global Accelerator](#).

Cara mengakses dan mengelola Route 53 Global Resolver melalui antarmuka AWS

Route 53 Global Resolver menyediakan beberapa metode akses untuk mengakomodasi preferensi manajemen dan persyaratan otomatisasi yang berbeda. Anda dapat mengelola Route 53 Global Resolver melalui antarmuka ini:

Konsol Manajemen AWS

Konsol Manajemen AWS Ini menyediakan antarmuka berbasis web untuk Route 53 Global Resolver. Anda dapat menggunakan konsol untuk mengonfigurasi kebijakan pemfilteran DNS, mengelola pengaturan autentikasi, dan memantau log kueri.

AWS Command Line Interface (AWS CLI)

AWS CLI Ini menyediakan akses langsung ke operasi Route 53 Global Resolver API. Anda dapat menggunakan AWS CLI untuk mengotomatiskan tugas Route 53 Global Resolver dan mengintegrasikannya ke dalam skrip dan alur kerja Anda.

AWS SDKs

AWS menyediakan SDKs banyak bahasa pemrograman. Anda dapat menggunakan SDKs untuk mengintegrasikan fungsionalitas Cloud Resolver ke dalam aplikasi Anda.

API REST

Route 53 Global Resolver menyediakan REST API yang dapat Anda gunakan untuk mengelola resolusi DNS dan kebijakan pemfilteran secara terprogram.

Didukung Wilayah AWS

Route 53 Global Resolver tersedia sebagai berikut: Wilayah AWS

- Wilayah AS Timur (N. Virginia)
- Wilayah US East (Ohio)
- Wilayah US West (N California)
- Wilayah US West (Oregon)
- Wilayah Eropa (Frankfurt)

- Wilayah Eropa (Irlandia)
- Wilayah Eropa (London)
- Wilayah Asia Pasifik (Mumbai)
- Wilayah Asia Pasifik (Singapura)
- Wilayah Asia Pasifik (Tokyo)
- Wilayah Asia Pasifik (Sydney)

Menyiapkan akses akun untuk Route 53 Global Resolver

Sebelum mulai menggunakan Route 53 Global Resolver, Anda memerlukan AWS akun dan izin yang sesuai untuk mengakses sumber daya Route 53 Global Resolver. Ini termasuk membuat pengguna dan peran IAM dengan izin yang diperlukan.

Bagian ini memandu Anda melalui langkah-langkah yang diperlukan untuk mengonfigurasi pengguna dan peran untuk mengakses Route 53 Global Resolver.

Topik

- [Mendaftar untuk Akun AWS](#)
- [Buat pengguna dengan akses administratif](#)
- [Membuat kebijakan dan peran](#)
- [Pertimbangan jaringan](#)

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat.

Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai

praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [Konsol Manajemen AWS](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Membuat kebijakan dan peran

Konfigurasi izin AWS Identity and Access Management (IAM) agar tim Anda dapat menerapkan dan mengelola sumber daya Route 53 Global Resolver. Anda dapat menggunakan izin administratif untuk akses penuh atau izin hanya-baca untuk memantau dan melihat konfigurasi.

Semua operasi Route 53 Global Resolver API memerlukan izin IAM yang sesuai. Jika Anda tidak memiliki izin yang diperlukan, panggilan API akan menampilkan kesalahan `AccessDeniedException (401)` atau `UnauthorizedException (401)`.

Izin administratif

Jika Anda menyiapkan Route 53 Global Resolver untuk pertama kalinya atau mengelola semua aspek layanan, Anda memerlukan izin administratif. Anda dapat menggunakan kebijakan AWS terkelola ini:

- `AmazonRoute53GlobalResolverFullAccess`- Menyediakan akses penuh ke sumber daya Route 53 Global Resolver, termasuk membuat, memperbarui, dan menghapus resolver global, tampilan DNS, aturan firewall, dan daftar domain
- `AmazonRoute53FullAccess`- Diperlukan jika Anda berencana untuk menggunakan penerusan zona host pribadi

- `CloudWatchLogsFullAccess`- Diperlukan jika Anda berencana untuk mengirim log ke Amazon CloudWatch
- `AmazonS3FullAccess`- Diperlukan jika Anda berencana untuk mengimpor daftar domain firewall dari Amazon S3 atau mengirim log ke Amazon S3

Izin baca-saja

Jika Anda hanya perlu melihat konfigurasi dan log Route 53 Global Resolver, Anda dapat menggunakan kebijakan terkelola ini AWS :

- `AmazonRoute53GlobalResolverReadOnlyAccess`- Menyediakan akses read-only ke sumber daya Route 53 Global Resolver, termasuk melihat resolver global, tampilan DNS, aturan firewall, daftar domain, dan sumber akses
- `AmazonRoute53ReadOnlyAccess`- Diperlukan untuk melihat asosiasi zona host pribadi
- `CloudWatchReadOnlyAccess`- Diperlukan untuk melihat log di Amazon CloudWatch
- `AmazonS3ReadOnlyAccess`- Diperlukan untuk melihat file daftar domain firewall yang disimpan di Amazon S3

Pertimbangan jaringan

Sebelum menerapkan Route 53 Global Resolver, pertimbangkan persyaratan jaringan berikut:

Rentang IP klien

Ini hanya diperlukan saat menggunakan otentikasi berbasis sumber akses. Identifikasi rentang alamat IP (blok CIDR) untuk semua klien yang akan menggunakan Route 53 Global Resolver. Anda akan memerlukan ini untuk mengonfigurasi aturan untuk sumber akses Anda.

Protokol DNS

Tentukan protokol DNS mana yang akan digunakan klien Anda:

- `Do53` - DNS standar melalui port 53 (UDP/TCP)
- `DoH` - DNS-over-HTTPS untuk kueri terenkripsi
- `DoT` - DNS-over-TLS untuk kueri terenkripsi

Firewall dan grup keamanan

Pastikan firewall jaringan dan grup keamanan Anda mengizinkan lalu lintas keluar ke Route 53 Global Resolver alamat IP anycast pada port yang sesuai (53 untuk Do53, 443 untuk DoH, 853 untuk DoT).

Tutorial: Buat Resolver Global Route 53 pertama Anda

Panduan memulai ini menunjukkan komponen dasar Route 53 Global Resolver dan secara opsional membuat pengaturan pemfilteran DNS sederhana. Tutorial ini mencakup konsep inti tetapi tidak termasuk persyaratan produksi seperti konfigurasi klien, logging, atau resolusi domain pribadi.

Setelah selesai, Anda akan memiliki pengaturan Route 53 Global Resolver dasar yang dapat memfilter kueri DNS dan memblokir domain berbahaya.

Bagian berikut menjelaskan cara cepat memulai dengan keamanan dan pemfilteran DNS menggunakan Route 53 Global Resolver.

Prasyarat

Sebelum Anda dapat menggunakan Route 53 Global Resolver, Anda memerlukan AWS akun dan izin yang sesuai untuk mengakses, melihat, dan mengedit komponen Route 53 Global Resolver.

Administrator sistem Anda harus menyelesaikan langkah-langkahnya [the section called “Menyiapkan akses akun”](#), dan kemudian kembali ke tutorial ini.

Langkah 1: Buat resolver global

Pertama, buat instance resolver global dan pilih AWS Wilayah tempat ia akan beroperasi.

1. Buka konsol Route 53 Global Resolver di <https://console.aws.amazon.com/route53globalresolver/>
2. Pilih Buat resolver global.
3. Untuk Nama, masukkan nama deskriptif untuk resolver global Anda.
4. Untuk Deskripsi, secara opsional masukkan deskripsi.
5. Untuk Wilayah, pilih dua atau lebih Wilayah AWS tempat Anda ingin membuat instance resolver global. Pilih Wilayah yang paling dekat dengan klien Anda untuk kinerja yang optimal.
6. Secara opsional, tambahkan tag untuk membantu mengatur dan mengelola sumber daya Anda.
7. Pilih Buat resolver global.

Anda akan segera menerima IPv4 alamat anycast yang dapat digunakan klien Anda untuk mencapai resolver. Proses pembuatan resolver global membutuhkan waktu beberapa menit untuk diselesaikan sebelum alamat menjadi fungsional.

Langkah 2: Buat tampilan DNS dan konfigurasi otentikasi

Buat tampilan DNS untuk mengatur klien Anda dan mengonfigurasi otentikasi menggunakan Sumber Akses IP. Tutorial ini menggunakan otentikasi berbasis IP. Anda juga dapat menggunakan token akses untuk protokol DOH/dot.

1. Di konsol Route 53 Global Resolver, pilih resolver global Anda.
2. Pilih Buat tampilan DNS.
3. Untuk Nama, masukkan nama deskriptif untuk tampilan DNS Anda.
4. Untuk Deskripsi, secara opsional masukkan deskripsi.
5. Pilih Buat tampilan DNS.
6. Setelah tampilan DNS dibuat, pilih Sumber akses dan kemudian Buat sumber akses.
7. Untuk blok CIDR, masukkan rentang alamat IP untuk klien Anda (misalnya, 203.0.113.0/24).
8. Untuk Protokol, pilih Do53 (DNS di atas port 53) untuk pengaturan dasar.
9. Pilih aturan Buat Sumber Akses.

Langkah 3: Konfigurasi aturan penyaringan DNS (opsional)

Siapkan aturan pemfilteran DNS dasar untuk memblokir akses ke domain berbahaya.

1. Dalam tampilan DNS Anda, pilih aturan Firewall dan kemudian Buat aturan firewall.
2. Untuk Nama, masukkan nama deskriptif untuk aturan.
3. Untuk Prioritas, masukkan 100 (angka yang lebih rendah memiliki prioritas lebih tinggi).
4. Untuk Tindakan, pilih Blokir.
5. Untuk jenis daftar Domain, pilih Daftar Domain AWS Terkelola.
6. Untuk daftar domain Terkelola, pilih AmazonGuardDutyThreatList dan Perintah dan Kontrol Malware dan Botnet untuk memblokir domain berbahaya yang diketahui (Anda dapat menambahkan daftar terkelola lainnya atau membuat daftar kustom nanti).
7. Pilih Buat aturan firewall.

Langkah 4: Uji konfigurasi Anda

Uji apakah konfigurasi Route 53 Global Resolver Anda berfungsi dengan benar.

1. Dari mesin klien dalam rentang CIDR yang dikonfigurasi, uji resolusi DNS menggunakan alamat IP anycast yang disediakan oleh resolver global Anda:

```
nslookup example.com <anycast-ip-address>
```

2. Verifikasi bahwa domain yang sah diselesaikan dengan benar.
3. Uji apakah domain yang diblokir difilter dengan benar. Anda dapat membuat daftar domain khusus dengan domain uji untuk memverifikasi aturan firewall Anda berfungsi dengan benar. Untuk informasi selengkapnya tentang Daftar Domain Terkelola, lihat [Daftar Domain Terkelola](#).
4. Periksa konsol Route 53 Global Resolver untuk log kueri dan aktivitas pemfilteran.

Untuk prosedur pengujian dan pemecahan masalah yang komprehensif, lihat Pemecahan Masalah Route 53 Global Resolver.

Langkah 5: Memantau aktivitas DNS

Konfigurasi logging untuk aktivitas DNS Anda.

1. Pilih Wilayah Observabilitas.
2. Pilih tujuan untuk log kueri.

Untuk prosedur pengujian dan pemecahan masalah yang komprehensif, lihat Menguji dan memecahkan masalah Route 53 Global Resolver.

Langkah 6: Bersihkan (opsional)

Jika Anda membuat konfigurasi ini untuk tujuan pengujian dan tidak ingin terus menggunakan Route 53 Global Resolver, bersihkan sumber daya untuk menghindari biaya yang sedang berlangsung.

1. Di konsol Route 53 Global Resolver, hapus semua aturan firewall yang Anda buat.
2. Hapus aturan Sumber Akses apa pun yang Anda buat.
3. Hapus tampilan DNS.
4. Hapus resolver global.

 Important

Menghapus sumber daya ini akan menghentikan resolusi DNS untuk setiap klien yang dikonfigurasi untuk menggunakannya. Perbarui konfigurasi klien Anda sebelum menghapus resolver atau menghapus aturan akses.

Langkah selanjutnya

Sekarang setelah Anda memiliki konfigurasi Route 53 Global Resolver dasar, Anda dapat menjelajahi fitur tambahan:

- Konfigurasi perangkat klien untuk menggunakan resolver Anda (diperlukan untuk produksi). Perbarui pengaturan DNS klien Anda untuk menggunakan alamat IP anycast yang disediakan oleh global resolver Anda.
- Atur pencatatan untuk pemantauan dan kepatuhan (direkomendasikan untuk produksi). Konfigurasi logging ke Amazon CloudWatch, Amazon S3, atau Amazon Data Firehose untuk pemantauan dan analisis. Untuk informasi selengkapnya, lihat [Memantau aktivitas dan kinerja DNS dengan Route 53 Global Resolver](#).
- Konfigurasi penerusan zona host pribadi untuk domain internal (diperlukan jika Anda memiliki sumber daya pribadi AWS). Untuk informasi selengkapnya, lihat [Menggunakan zona yang di-hosting pribadi](#).
- Siapkan konektivitas DNS terenkripsi menggunakan DNS-over-HTTPS (DoH) atau DNS-over-TLS (DoT). Untuk informasi selengkapnya, lihat [Mengonfigurasi DNS terenkripsi](#).
- Buat daftar domain khusus dan aturan pemfilteran tingkat lanjut. Untuk informasi selengkapnya, lihat [Pemfilteran DNS](#).

Mengelola tampilan DNS dengan Route 53 Global Resolver

Anda dapat mengelola operasi Route 53 Global Resolver yang sedang berlangsung termasuk memperbarui tampilan DNS untuk mengontrol grup perangkat klien mana yang dapat diselesaikan ke sumber daya internal dan domain apa yang akan difilter.

Mengelola tampilan DNS

Setelah membuat tampilan DNS, Anda dapat memperbarui konfigurasinya, mengaktifkan atau menonaktifkannya, dan mengelola siklus hidupnya.

Membuat tampilan DNS untuk grup perangkat klien

Tampilan DNS adalah pengelompokan logis yang mendefinisikan kebijakan keamanan untuk sekelompok perangkat klien, seperti pekerja jarak jauh, perangkat kantor cabang, atau peralatan lokal. Setiap tampilan memiliki persyaratan otentikasi sendiri, aturan pemfilteran, dan asosiasi zona host pribadi.

Untuk membuat tampilan DNS

1. Buka konsol di <https://console.aws.amazon.com/route53globalresolver/>.
2. Pilih resolver global Anda dari daftar.
3. Pilih tab tampilan DNS.
4. Pilih Buat tampilan DNS.
5. Di bagian detail tampilan DNS:
 - a. Untuk nama tampilan DNS, masukkan nama deskriptif untuk tampilan DNS Anda (hingga 128 karakter).
 - b. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk tampilan DNS Anda (hingga 255 karakter).
6. Di bagian penanganan kueri DNS, konfigurasi pengaturan berikut:
 - Validasi DNSSEC - Pilih Aktifkan atau Nonaktifkan. Validasi DNSSEC memungkinkan Global Resolver untuk memverifikasi keaslian respons DNS.
 - Aturan firewall gagal membuka perilaku - Pilih Aktifkan untuk mengizinkan kueri dilanjutkan ketika DNS Firewall tidak dapat mengevaluasinya, atau Nonaktifkan untuk memblokir kueri tersebut.
 - Subnet klien EDNS0 - Pilih Aktifkan untuk meningkatkan akurasi lokasi klien untuk perutean lalu lintas ke sumber daya terdekat dan caching yang efisien, atau Nonaktifkan untuk mematikan fitur ini.
7. Pilih Buat tampilan DNS.

Setelah membuat tampilan DNS, Anda dapat mengonfigurasi kontrol akses, aturan firewall, dan asosiasi zona host pribadi.

Mengedit tampilan DNS

Anda dapat mengubah pengaturan tampilan DNS setelah pembuatan, termasuk opsi penanganan kueri DNS dan sumber daya terkait.

Untuk mengedit tampilan DNS

1. Di konsol, arahkan ke resolver global Anda.
2. Pilih tab tampilan DNS.
3. Pilih tampilan DNS yang ingin Anda edit dan pilih Edit.
4. Ubah pengaturan tampilan DNS sesuai kebutuhan dan pilih Simpan perubahan.

Mengaktifkan dan menonaktifkan tampilan DNS

Anda dapat menonaktifkan sementara tampilan DNS tanpa menghapusnya. Saat dinonaktifkan, penyelesaian global berhenti melayani permintaan untuk perangkat klien yang terkait dengan tampilan DNS tersebut.

Warning

Menonaktifkan tampilan DNS segera menghentikan resolusi DNS untuk semua perangkat klien yang terkait dengan tampilan itu. Pastikan Anda memiliki resolusi DNS alternatif yang dikonfigurasi untuk perangkat klien yang terpengaruh.

Menghapus tampilan DNS

Sebelum Anda dapat menghapus tampilan DNS, Anda harus terlebih dahulu menghapus semua sumber daya terkait, termasuk aturan Sumber Akses, token akses, aturan firewall, dan asosiasi zona yang dihosting pribadi.

Warning

Menghapus tampilan DNS tidak dapat diubah dan akan segera menghentikan resolusi DNS untuk semua perangkat klien yang terkait dengan tampilan itu.

Mengelola asosiasi zona yang dihosting pribadi

Anda dapat melihat, memperbarui, dan menghapus asosiasi zona yang dihosting pribadi sesuai kebutuhan untuk mengontrol grup perangkat klien mana yang memiliki akses ke sumber daya internal.

Melihat asosiasi

Untuk melihat semua asosiasi zona yang dihosting pribadi untuk tampilan DNS, navigasikan ke tampilan DNS Anda dan periksa bagian Zona yang dihosting pribadi untuk melihat semua zona terkait dengan status dan detail asosiasi mereka.

Memperbarui asosiasi

Anda dapat memperbarui nama asosiasi zona yang dihosting pribadi dengan memilih asosiasi, memilih Edit, memperbarui nama asosiasi, dan menyimpan perubahan.

Menghapus asosiasi

Saat Anda menghapus asosiasi zona yang dihosting pribadi, Route 53 Global Resolver berhenti menggunakan zona tersebut untuk menyelesaikan kueri DNS untuk tampilan DNS terkait.

Warning

Menghapus asosiasi zona yang dihosting pribadi segera memengaruhi resolusi DNS. Kueri untuk domain di zona terputus akan diselesaikan menggunakan DNS publik, bukan catatan zona pribadi.

Konfigurasi pengaturan untuk tampilan DNS di Route 53 Global Resolver

Route 53 Global Resolver memungkinkan Anda mengonfigurasi kebijakan DNS dan kontrol akses yang berbeda untuk grup perangkat klien yang berbeda berdasarkan persyaratan keamanan dan kebutuhan akses mereka. Siapkan kebijakan DNS dan kontrol akses di Route 53 Global Resolver untuk berbagai grup perangkat klien berdasarkan persyaratan keamanan dan kebutuhan akses mereka.

Mengkonfigurasi pengaturan DNS untuk grup klien

Setiap tampilan DNS memiliki beberapa pengaturan yang mengontrol bagaimana kueri DNS diproses dan diselesaikan untuk grup perangkat klien yang berbeda.

Validasi DNSSEC

Validasi DNSSEC membantu memastikan bahwa respons DNS untuk domain publik adalah otentik dan belum dirusak. Saat Anda mengaktifkan validasi DNSSEC, Route 53 Global Resolver memeriksa tanda tangan DNSSEC dan mengembalikan SERVFAIL untuk domain dengan tanda tangan tidak valid.

Pertimbangkan untuk mengaktifkan validasi DNSSEC jika:

- Organisasi Anda memerlukan verifikasi kriptografi tanggapan DNS
- Anda menginginkan perlindungan terhadap spoofing DNS dan serangan keracunan cache
- Anda memiliki persyaratan kepatuhan yang memerlukan validasi DNSSEC

Note

Validasi DNSSEC hanya berlaku untuk domain publik. Zona yang dihosting pribadi menggunakan mekanisme otentikasi mereka sendiri.

Subnet Klien EDNS (ECS)

EDNS Client Subnet mencakup informasi tentang lokasi jaringan klien dalam kueri DNS yang dikirim ke server otoritatif. Hal ini memungkinkan jaringan pengiriman konten dan layanan yang didistribusikan secara geografis untuk memberikan tanggapan yang sesuai lokasi.

ECS dapat membantu Anda:

- Dapatkan kinerja yang lebih baik dari layanan yang didistribusikan secara geografis
- Meningkatkan akurasi perutean jaringan pengiriman konten
- Lebih baik mematuhi pembatasan konten regional

Pertimbangan privasi:

- ECS mengungkapkan sebagian informasi IP klien ke server otoritatif (maksimum/24 untuk IPv4 dan /48 untuk IPv6)
- Pertimbangkan persyaratan privasi organisasi Anda sebelum mengaktifkan

Firewall gagal terbuka

Firewall gagal membuka pengaturan menentukan apa yang terjadi ketika aturan firewall DNS tidak dapat dievaluasi karena gangguan layanan atau masalah konfigurasi.

Dinonaktifkan (default)

Kueri DNS diblokir ketika aturan firewall tidak dapat dievaluasi. Ini memberi Anda keamanan maksimum tetapi dapat memengaruhi ketersediaan selama masalah layanan.

Diaktifkan

Kueri DNS diperbolehkan ketika aturan firewall tidak dapat dievaluasi. Ini memprioritaskan ketersediaan daripada keamanan selama masalah layanan.

Praktik terbaik untuk mengatur grup perangkat klien

Ikuti praktik terbaik ini saat mendesain tampilan DNS untuk grup perangkat klien yang berbeda:

Lihat strategi organisasi

- Pisahkan dengan persyaratan keamanan - Buat tampilan berbeda untuk perangkat klien dengan izin keamanan atau tingkat akses yang berbeda
- Atur berdasarkan lokasi - Gunakan tampilan terpisah untuk lokasi geografis atau segmen jaringan yang berbeda
- Kelompokkan berdasarkan jenis perangkat - Buat tampilan khusus untuk server, workstation, perangkat seluler, atau perangkat IoT
- Gunakan nama deskriptif - Pilih nama yang secara jelas menunjukkan tujuan tampilan dan perangkat klien target

Pertimbangan keamanan

- Prinsip hak istimewa terkecil - Konfigurasi setiap tampilan dengan akses minimum yang diperlukan untuk perangkat kliennya
- Default deny - Mulai dengan aturan firewall terbatas dan tambahkan pengecualian sesuai kebutuhan
- Tinjauan rutin - Tinjau dan perbarui konfigurasi tampilan DNS secara berkala
- Memantau penggunaan - Gunakan log kueri DNS untuk memantau dan menganalisis pola penggunaan tampilan DNS

Mengelola kontrol akses dengan sumber akses dan token di Route 53 Global Resolver

Route 53 Global Resolver menyediakan dua metode utama untuk mengontrol akses perangkat klien: sumber akses untuk otentikasi berbasis IP dan token akses untuk otentikasi berbasis token. Bab ini mencakup kedua pendekatan, membantu Anda memilih metode otentikasi yang tepat untuk lingkungan Anda dan menerapkan kontrol akses yang komprehensif.

Topik

- [Memahami metode kontrol akses di Route 53 Global Resolver](#)
- [Mengkonfigurasi sumber akses dan aturan sumber akses](#)
- [Mengelola token akses untuk otentikasi terenkripsi](#)
- [Praktik terbaik kontrol akses dan pertimbangan keamanan](#)

Memahami metode kontrol akses di Route 53 Global Resolver

Route 53 Global Resolver menawarkan dua metode otentikasi berbeda untuk mengontrol akses klien ke infrastruktur DNS Anda. Setiap metode melayani kasus penggunaan dan lingkungan yang berbeda.

Sumber akses berbasis IP

Anda mengonfigurasi aturan sumber akses yang mengizinkan atau menolak kueri DNS berdasarkan alamat IP klien. Metode ini bekerja dengan baik untuk lingkungan dengan rentang IP yang dapat diprediksi, seperti kantor cabang atau koneksi VPN. Sumber akses mendukung semua protokol DNS (Do53, DoT, dan DoH) dan menyediakan konfigurasi langsung untuk administrator jaringan.

Otentikasi berbasis token

Token akses menyediakan otentikasi aman untuk protokol DoH dan DoT menggunakan kredensial terenkripsi dan terbatas waktu. Metode ini sesuai dengan klien seluler dan lingkungan di mana alamat IP sering berubah. Anda dapat memperbarui token sebelum kedaluwarsa dan mereka menawarkan keamanan yang ditingkatkan melalui enkripsi.

Pertimbangkan faktor-faktor ini saat memilih pendekatan otentikasi Anda:

Memilih metode otentikasi yang tepat

Faktor	Sumber akses	Token akses
Terbaik untuk	Rentang IP tetap, jaringan kantor, pengguna VPN	Perangkat seluler, dinamis IPs, pekerja jarak jauh
Tingkat keamanan	Berbasis jaringan, bergantung pada kepercayaan IP	Kredensi terenkripsi, terbatas waktu
Kompleksitas manajemen	Manajemen rentang IP sederhana	Siklus hidup dan distribusi Token
Dukungan protokol	Do53, DoT, DoH	DoT, hanya DoH

Anda dapat menggunakan kedua metode secara bersamaan untuk membuat keamanan berlapis. Misalnya, gunakan sumber akses untuk jaringan kantor dan token untuk pekerja jarak jauh.

Mengkonfigurasi sumber akses dan aturan sumber akses

Sumber akses mengontrol akses klien berdasarkan alamat IP. Anda membuat aturan sumber akses yang menentukan rentang IP mana yang dapat menanyakan infrastruktur DNS Anda dan protokol mana yang dapat mereka gunakan.

Membuat aturan sumber akses

Ikuti langkah-langkah ini untuk membuat aturan sumber akses yang memungkinkan rentang IP tertentu untuk menanyakan infrastruktur DNS Anda.

1. Buka konsol Route 53 Global Resolver dan navigasikan ke tampilan DNS Anda.
2. Di bagian Sumber akses, pilih Buat aturan sumber akses.
3. Untuk Nama, masukkan nama deskriptif yang mengidentifikasi tujuan aturan ini, seperti `office-network` atau `vpn-users`.
4. Untuk rentang alamat IP, tentukan alamat IP yang seharusnya memiliki akses. Anda dapat menggunakan notasi CIDR untuk rentang IP: `192.168.1.0/24` atau alamat IP individual: `203.0.113.5/32`.
5. Untuk Protokol, pilih protokol DNS aturan ini berlaku untuk:

- Do53 - DNS standar di atas UDP/TCP (port 53)
- DoT - DNS melalui TLS (port 853)
- DoH - DNS melalui HTTPS (port 443)

6. Pilih Buat aturan sumber akses.

Perangkat klien dari rentang IP yang ditentukan sekarang dapat menanyakan infrastruktur DNS Anda menggunakan protokol yang dipilih.

Memahami evaluasi aturan dan prioritas

Route 53 Global Resolver mengevaluasi aturan sumber akses saat mengidentifikasi tampilan yang benar untuk digunakan.

- Aturan diproses dari rentang IP yang paling spesifik hingga yang paling tidak spesifik, di mana aturan pencocokan paling spesifik diutamakan.
- Jika tidak ada aturan yang cocok, permintaan ditolak secara default.

Uji konfigurasi sumber akses Anda dengan menanyakan dari alamat IP yang berbeda untuk memastikan aturan berfungsi seperti yang diharapkan.

Mengelola token akses untuk otentikasi terenkripsi

Token akses menyediakan otentikasi terenkripsi untuk protokol DoH dan DoT. Tidak seperti sumber akses berbasis IP, token bekerja terlepas dari lokasi klien dan menawarkan keamanan yang ditingkatkan melalui enkripsi dan kontrol kedaluwarsa.

Membuat token akses

Ikuti langkah-langkah ini untuk membuat token akses untuk mengautentikasi perangkat klien yang menggunakan protokol DoH atau DoT.

1. Buka konsol Route 53 Global Resolver dan navigasikan ke tampilan DNS Anda.
2. Di bagian Sumber akses, pilih Buat token akses.
3. Untuk Nama, masukkan nama deskriptif yang mengidentifikasi tujuan token, seperti `mobile-devices` atau `remote-workers-q4`

4. Untuk Kedaluwarsa, atur kapan token harus kedaluwarsa. Kami merekomendasikan 90 hari atau kurang untuk keamanan. Pertimbangkan distribusi token dan kemampuan perpanjangan Anda saat mengatur periode kedaluwarsa.
5. Pilih Buat token akses.
6. Distribusikan token dengan aman ke perangkat klien Anda menggunakan saluran komunikasi aman organisasi Anda.

Mengkonfigurasi perangkat klien dengan token akses

Konfigurasi perangkat klien untuk menggunakan token akses untuk otentikasi dengan infrastruktur Route 53 Global Resolver Anda.

konfigurasi DoH

Untuk mengonfigurasi DoH dengan token akses, Anda memerlukan nama DNS atau alamat IP resolver global Anda:

1. Gunakan GetGlobalResolver API untuk mengambil detail konektivitas untuk resolver Anda.
2. Perhatikan `ipv4Addresses` (misalnya, 3.3.3.3, 3.3.3.4) dan (misalnya, `dnsName a1bc234567890a.route53globalresolver.global.on.aws`).
3. Sertakan token sebagai parameter URL di titik akhir DoH menggunakan nama DNS:

```
https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<token-value>
```

Ganti `<token-value>` dengan token aktual yang Anda hasilkan.

Konfigurasi DoT

Untuk kueri DoT dengan token akses, sertakan token dalam opsi EDNS0 dengan spesifikasi berikut:

- Kode Opsi: `0xffa0`
- Data Opsi: Token akses dalam format string

Implementasi spesifik tergantung pada perangkat lunak klien DoT Anda dan bagaimana menangani opsi EDNS0.

Manajemen siklus hidup token

Kelola kedaluwarsa dan pembaruan token untuk menjaga akses aman untuk perangkat klien Anda.

- Pantau tanggal kedaluwarsa - Lacak tanggal kedaluwarsa token dan rencanakan perpanjangan terlebih dahulu.
- Perpanjang sebelum kedaluwarsa - Buat token baru sebelum yang lama kedaluwarsa untuk menghindari gangguan layanan.
- Putar token secara teratur - Ganti token secara berkala bahkan sebelum kedaluwarsa untuk keamanan yang ditingkatkan.
- Cabut token yang dikompromikan - Hapus token segera jika Anda mencurigai token tersebut telah disusupi.

Pertimbangkan untuk menerapkan proses pembaruan token otomatis untuk penerapan besar guna mengurangi overhead administratif.

Contoh konfigurasi platform

Gunakan contoh khusus platform ini untuk mengonfigurasi perangkat klien dengan token akses Route 53 Global Resolver dan detail koneksi Anda.

Konfigurasi Windows

Ikuti langkah-langkah ini untuk mengkonfigurasi klien Windows untuk menggunakan DoH dengan token akses menggunakan perintah netsh.

1. Buka Command Prompt sebagai administrator.
2. Aktifkan setelan DoH global:

```
netsh dns add global doh=yes
```

3. Daftarkan server DoH dengan token akses. Ganti nilai contoh dengan detail resolver Anda yang sebenarnya:

```
netsh dns add encryption server=3.3.3.3 dohtemplate=https://  
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>  
autoupgrade=yes
```

```
netsh dns add encryption server=3.3.3.4 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
autoupgrade=yes
```

4. Siram cache DNS:

```
ipconfig /flushdns
```

5. Verifikasi konfigurasi:

```
netsh dns show global
```

konfigurasi macOS

Ikuti langkah-langkah berikut untuk mengonfigurasi klien macOS menggunakan profil konfigurasi seluler untuk DoH dengan token akses.

Buat profil konfigurasi seluler dengan struktur berikut:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>DNSSettings</key>
      <dict>
        <key>DNSProtocol</key>
        <string>HTTPS</string>
        <key>ServerAddresses</key>
        <array>
          <string>3.3.3.3</string>
          <string>3.3.3.4</string>
        </array>
        <key>ServerURL</key>
        <string>https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?
token=<your-token></string>
      </dict>
      <key>PayloadType</key>
      <string>com.apple.dnsSettings.managed</string>
    </dict>
  </array>
</dict>
```

```
</dict>
</array>
</dict>
</plist>
```

Instal profil melalui Pengaturan Sistem > Manajemen Perangkat.

Praktik terbaik kontrol akses dan pertimbangan keamanan

Ikuti praktik terbaik ini untuk menjaga kontrol akses yang aman dan efektif untuk infrastruktur Route 53 Global Resolver Anda.

Praktik terbaik keamanan

Terapkan langkah-langkah keamanan ini untuk melindungi infrastruktur DNS Anda:

- Gunakan otentikasi berlapis - Gabungkan sumber akses untuk jaringan tepercaya dengan token untuk pengguna seluler. Pendekatan ini memberikan pertahanan secara mendalam dan mengakomodasi skenario klien yang berbeda.
- Terapkan akses hak istimewa paling sedikit - Berikan akses hanya ke rentang IP dan protokol yang benar-benar dibutuhkan klien. Hindari aturan sumber akses yang terlalu luas yang dapat mengekspos infrastruktur Anda untuk penggunaan yang tidak sah.
- Putar token secara teratur - Ganti token akses pada jadwal reguler, bahkan sebelum kedaluwarsa. Praktik ini membatasi dampak token yang dikompromikan dan menjaga kebersihan keamanan.
- Pantau pola akses - Tinjau log kueri DNS untuk mengidentifikasi pola akses yang tidak biasa atau potensi masalah keamanan. Siapkan peringatan untuk kueri dari rentang IP yang tidak terduga atau menggunakan token kedaluwarsa.

Praktik terbaik operasional

Ikuti praktik operasional ini untuk mempertahankan kontrol akses yang andal:

- Dokumentasikan strategi kontrol akses Anda - Pertahankan dokumentasi yang jelas tentang sumber akses dan token mana yang melayani grup klien mana.
- Uji kontrol akses secara teratur - Verifikasi bahwa aturan dan token sumber akses Anda berfungsi dengan benar dari lokasi dan skenario klien yang berbeda.
- Rencanakan pembaruan token - Tetapkan proses untuk mendistribusikan token baru sebelum token lama kedaluwarsa untuk menghindari gangguan layanan.

- Tinjau kontrol akses secara berkala - Hapus aturan sumber akses yang tidak digunakan dan token kedaluwarsa untuk mempertahankan konfigurasi yang bersih.

Mengamankan DNS untuk klien dengan Route 53 Global Resolver

Bagian berikut menjelaskan cara membuat aturan untuk mengamankan kueri DNS yang dibuat oleh klien Anda.

Topik

- [Konfigurasi dan kelola aturan DNS Firewall](#)
- [Daftar Domain Terkelola untuk Route 53 Global Resolver](#)
- [Buat daftar domain untuk diblokir atau diizinkan](#)
- [Perlindungan tingkat lanjut DNS Firewall](#)
- [Mengelola kebijakan keamanan DNS di Route 53 Global Resolver](#)

Konfigurasi dan kelola aturan DNS Firewall

Membuat dan melihat aturan firewall

Aturan firewall menentukan cara Route 53 Global Resolver menangani kueri DNS berdasarkan daftar domain, daftar domain terkelola, kategori konten, atau perlindungan ancaman lanjutan. Setiap aturan menentukan prioritas, domain target, dan tindakan yang harus diambil.

Praktik terbaik untuk prioritas aturan:

- Gunakan prioritas 100-999 untuk aturan izin prioritas tinggi (domain tepercaya)
- Gunakan prioritas 1000-4999 untuk aturan blok (ancaman yang diketahui)
- Gunakan prioritas 5000-9999 untuk aturan peringatan (pemantauan dan analisis)
- Tinggalkan celah di antara prioritas untuk memungkinkan penyisipan aturan di masa depan

Untuk membuat aturan DNS Firewall

1. Di konsol Route 53 Global Resolver, navigasikan ke tampilan DNS Anda.
2. Pilih tab Aturan Firewall.

3. Pilih Buat aturan firewall.
4. Di bagian Rincian aturan:
 - a. Untuk nama Aturan, masukkan nama deskriptif untuk aturan (hingga 128 karakter).
 - b. (Opsional) Untuk deskripsi Aturan, masukkan deskripsi untuk aturan (hingga 255 karakter).
5. Di bagian konfigurasi Aturan, pilih tipe konfigurasi Aturan:
 - Daftar domain terkelola pelanggan - Gunakan daftar domain yang Anda buat dan kelola
 - AWS daftar domain terkelola - Gunakan daftar domain yang disediakan oleh Amazon yang dapat Anda manfaatkan
 - Perlindungan lanjutan DNS Firewall - Pilih dari berbagai perlindungan terkelola dan tentukan ambang batas kepercayaan
6. Untuk tindakan Aturan, pilih tindakan yang akan diambil ketika aturan cocok:
 - Izinkan - Kueri DNS diselesaikan
 - Peringatan - Memungkinkan kueri DNS tetapi membuat peringatan
 - Blokir - Kueri DNS diblokir
7. Pilih Buat aturan firewall.

Gunakan prosedur berikut untuk melihat aturan yang ditetapkan untuk mereka. Anda juga dapat memperbarui pengaturan aturan dan aturan.

Untuk melihat dan memperbarui aturan

1. Di konsol Route 53 Global Resolver, navigasikan ke Tampilan DNS Anda.
2. Pilih tab Aturan DNS Firewall.
3. Pilih aturan yang ingin Anda lihat atau edit, dan pilih Edit.
4. Di halaman Aturan, Anda dapat melihat dan mengedit pengaturan.

Untuk informasi tentang nilai aturan, lihat [the section called “Pengaturan aturan di DNS Firewall”](#).

Untuk menghapus aturan

1. Di konsol Route 53 Global Resolver, navigasikan ke Tampilan DNS Anda.
2. Pilih tab Aturan DNS Firewall.
3. Pilih aturan yang ingin Anda hapus, lalu pilih Hapus, dan konfirmasi penghapusan.

Pengaturan aturan di DNS Firewall

Saat membuat atau mengedit aturan DNS Firewall di Tampilan DNS, Anda menentukan nilai berikut:

Nama

Pengidentifikasi unik untuk aturan dalam Tampilan DNS.

Deskripsi (Opsional)

Deskripsi singkat yang memberikan informasi lebih lanjut tentang aturan.

Daftar domain

Daftar domain yang diperiksa oleh aturan. Anda dapat membuat dan mengelola daftar domain Anda sendiri atau Anda dapat berlangganan daftar domain yang AWS mengelola untuk Anda.

Aturan dapat berisi eter daftar domain atau perlindungan DNS Firewall Advanced, tetapi tidak keduanya.

Jenis kueri (hanya daftar domain)

Daftar jenis kueri DNS yang diperiksa aturan. Berikut ini adalah nilai yang valid:

- A: Mengembalikan IPv4 alamat.
- AAAA: Mengembalikan alamat Ipv6.
- CAA: Membatasi CAs yang dapat membuat SSL/TLS sertifikasi untuk domain.
- CNAME: Mengembalikan nama domain lain.
- DS: Rekam yang mengidentifikasi kunci penandatanganan DNSSEC dari zona yang didelegasikan.
- MX: Menentukan server email.
- NAPTR: Regular-expression-based menulis ulang nama domain.
- NS: Server nama otoritatif.
- PTR: Memetakan alamat IP ke nama domain.
- SOA: Mulai dari catatan otoritas untuk zona tersebut.
- SPF: Daftar server yang berwenang untuk mengirim email dari domain.
- SRV: Nilai spesifik aplikasi yang mengidentifikasi server.
- TXT: Memverifikasi pengirim email dan nilai khusus aplikasi.

Jenis kueri yang Anda tentukan dengan menggunakan ID tipe DNS, misalnya 28 untuk AAAA. Nilai harus didefinisikan sebagai TYPENUMBER, di mana NUMBER bisa 1-65334, misalnya, TYPE28 Untuk informasi selengkapnya, lihat [Daftar jenis rekaman DNS](#).

Anda dapat membuat satu jenis kueri per aturan.

DNS Firewall Perlindungan tingkat lanjut

Mendeteksi kueri DNS yang mencurigakan berdasarkan tanda tangan ancaman yang diketahui dalam kueri DNS. Anda dapat memilih perlindungan dari:

- Algoritma Pembuatan Domain () DGAs

DGAs digunakan oleh penyerang untuk menghasilkan sejumlah besar domain untuk meluncurkan serangan malware.

- Terowongan DNS

Tunneling DNS digunakan oleh penyerang untuk mengekstraksi data dari klien dengan menggunakan terowongan DNS tanpa membuat koneksi jaringan ke klien.

Dalam aturan DNS Firewall Advanced Anda dapat memilih untuk memblokir, atau memperingatkan pada kueri yang cocok dengan ancaman.

Untuk informasi selengkapnya, lihat Perlindungan DNS Firewall Advanced.

Aturan dapat berisi eter perlindungan DNS Firewall Advanced atau daftar domain, tetapi tidak keduanya.

Ambang kepercayaan (DNS Firewall Advanced saja)

Ambang batas kepercayaan untuk DNS Firewall Advanced. Nilai ini harus diisi saat membuat aturan DNS Firewall Advanced. Nilai tingkat kepercayaan berarti:

- Tinggi – Hanya mendeteksi ancaman yang telah dikonfirmasi dengan tingkat false positive yang rendah.
- Sedang – Menyediakan keseimbangan antara deteksi ancaman dan false positive.
- Rendah – Memberikan tingkat deteksi tertinggi untuk ancaman, tetapi juga meningkatkan false positive.

Untuk informasi selengkapnya, lihat Pengaturan aturan di DNS Firewall.

Tindakan

Bagaimana Anda ingin DNS Firewall menangani kueri DNS yang nama domainnya cocok dengan spesifikasi dalam daftar domain aturan. Untuk informasi selengkapnya, lihat [the section called “Aturan tindakan di DNS Firewall”](#).

Prioritas

Pengaturan bilangan bulat positif unik untuk aturan dalam Tampilan DNS yang menentukan urutan pemrosesan. DNS Firewall memeriksa kueri DNS terhadap aturan dalam Tampilan DNS dimulai dengan pengaturan prioritas numerik terendah dan naik. Anda dapat mengubah prioritas aturan kapan saja, misalnya mengubah urutan pemrosesan atau memberi ruang untuk aturan lain.

Aturan tindakan di DNS Firewall

Saat DNS Firewall menemukan kecocokan antara kueri DNS dan spesifikasi domain dalam aturan, hal ini menerapkan tindakan yang ditentukan dalam aturan ke kueri.

Anda harus menentukan salah satu opsi berikut di setiap aturan yang Anda buat:

- Izinkan — Berhenti memeriksa kueri dan membiarkannya melewatinya. Tidak tersedia untuk DNS Firewall Advanced.
- Peringatan — Berhenti memeriksa kueri, mengizinkannya masuk, dan catat peringatan untuk kueri di log Route 53 Resolver.
- Blokir — Hentikan pemeriksaan kueri, blokir agar tidak pergi ke tujuan yang diinginkan, dan catat tindakan blok untuk kueri di log Route 53 Resolver.

Balas dengan respons blok yang dikonfigurasi, dari berikut ini:

- NODATA — Menanggapi yang menunjukkan bahwa kueri berhasil, tetapi tidak ada respons yang tersedia untuk itu.
- NXDOMAIN — Menanggapi yang menunjukkan bahwa nama domain kueri tidak ada.
- OVERRIDE - Berikan penggantian khusus dalam respons. Opsi ini memerlukan pengaturan tambahan sebagai berikut:
 - Nilai rekam — Catatan DNS kustom untuk dikirim kembali sebagai respons terhadap kueri.
 - Jenis rekaman — Jenis catatan DNS. Ini akan menentukan format nilai catatan. Ini harus CNAME.

- Waktu untuk hidup dalam hitungan detik — Jumlah waktu yang disarankan untuk penyelesai DNS atau browser web untuk menyimpan catatan penggantian dan menggunakannya sebagai respons terhadap kueri ini, jika diterima lagi. Secara default, ini adalah nol, dan catatan tidak di-cache.

Daftar Domain Terkelola untuk Route 53 Global Resolver

Daftar Domain Terkelola berisi nama domain yang terkait dengan aktivitas berbahaya atau potensi ancaman lainnya. AWS memelihara daftar ini untuk memungkinkan pelanggan Route 53 Global Resolver memeriksa kueri DNS terikat internet terhadap mereka saat menggunakan DNS Firewall.

Terus memantau kondisi terbaru terkait lanskap ancaman yang terus berubah dapat memakan waktu dan biaya yang besar. Daftar Domain Terkelola dapat menghemat waktu Anda saat menerapkan dan menggunakan DNS Firewall di Global Resolver. AWS secara otomatis memperbarui daftar ketika kerentanan dan ancaman baru muncul.

Daftar domain terkelola dikategorikan ke dalam kategori Ancaman dan Konten, dirancang untuk membantu melindungi Anda dari ancaman web umum dan juga memblokir resolusi kueri ke domain bukan safe-for-work.

Sebagai praktik terbaik, sebelum menggunakan Daftar Domain Terkelola dalam produksi, ujilah di lingkungan non-produksi, dengan tindakan aturan disetel ke `Alert`. Evaluasi aturan menggunakan CloudWatch metrik Amazon yang dikombinasikan dengan permintaan sampel DNS Firewall atau log Resolver Global. Saat Anda puas bahwa aturan melakukan apa yang Anda inginkan, ubah setelan tindakan sesuai kebutuhan.

Daftar Domain AWS Terkelola yang Tersedia

Bagian ini menjelaskan Daftar Domain Terkelola yang saat ini tersedia untuk Resolver Global. AWS menyediakan Daftar Domain Terkelola berikut, untuk semua pengguna Global Resolver, diklasifikasikan berdasarkan Ancaman atau Jenis Konten.

Kategori Ancaman

Malware

Botnet/Perintah dan Kontrol

Daftar Ancaman Agregat

Daftar GuardDuty Ancaman Amazon

Phishing

Spam

Kategori Konten

Kekerasan dan Pidato Kebencian

Untuk Anak-Anak

Iklan Online

Sains

Keluarga dan Parenting

Hewan peliharaan

Karir dan Pencarian Pekerjaan

Agama

Gaya hidup

Rumah dan Taman

Aktivitas Kriminal dan Ilegal

Olahraga dan Rekreasi

Kendaraan

Layanan Keuangan

Real Estat

Hobi dan Minat

Perjalanan

Makanan dan Makan

Pemerintah dan Hukum

Edukasi

Mode

Health

Belanja

Konten Dewasa dan Dewasa

Teknologi dan Internet

Bisnis dan Ekonomi

Berita

Mesin Pencari dan Portal

Seni dan Budaya

Hiburan

Militer

Jejaring Sosial

Penghindaran Proksi

Mengalihkan

Email

Terjemahan

Pelecehan Anak

Aborsi

Judi

Peretasan

Ganja

Mata Uang Kripto

Kencan

Kecerdasan Buatan dan Machine Learning

Domain yang diparkir

Alamat IP Pribadi

Daftar Domain Terkelola tidak dapat diunduh atau dijelajahi. Untuk melindungi kekayaan intelektual, Anda tidak dapat melihat atau mengedit spesifikasi domain individual dalam Daftar Domain Terkelola. Pembatasan ini juga membantu mencegah pengguna jahat merancang ancaman yang secara khusus menghindari daftar yang dipublikasikan.

Buat daftar domain untuk diblokir atau diizinkan

Anda dapat membuat daftar domain Anda sendiri untuk menentukan kategori domain yang tidak Anda temukan di penawaran daftar domain terkelola atau yang Anda pilih untuk tangani sendiri.

Selain prosedur yang dijelaskan di bagian ini, di konsol, Anda dapat membuat daftar domain dalam konteks manajemen aturan DNS Firewall, saat Anda membuat atau memperbarui aturan.

Setiap spesifikasi domain dalam daftar domain Anda harus memenuhi persyaratan berikut:

- Secara opsional dapat diawali dengan * (tanda bintang).
- Dengan pengecualian tanda bintang awal opsional dan titik, sebagai pembatas antara label, itu hanya boleh berisi karakter berikut: A-Z, a-z 0-9, - (tanda hubung).
- Panjangnya harus antara 1-255 karakter.

Untuk membuat daftar domain

1. Di konsol Route 53 Global Resolver, navigasikan ke Global Resolver Anda.

2. Pilih tab Daftar domain.
3. Pilih Buat daftar domain.
4. Berikan nama dan deskripsi opsional untuk daftar domain Anda, bersama dengan tag apa pun, dan pilih Buat daftar domain.
5. Setelah dibuat dan beroperasi, Anda dapat mulai menambahkan domain ke daftar domain Anda dengan memilih Tambahkan domain.
6. Jika Anda memilih untuk Mengunggah daftar domain dari bucket Amazon S3, masukkan URI bucket Amazon S3 tempat Anda membuat daftar domain. Daftar domain ini harus memiliki satu nama domain per baris.
7. Jika tidak, masukkan spesifikasi domain Anda di kotak teks, satu per baris.
8. Pilih Tambahkan domain.

Untuk menghapus daftar domain

1. Di konsol Route 53 Global Resolver, navigasikan ke Global Resolver Anda.
2. Pilih tab Daftar domain.
3. Pilih daftar domain yang ingin Anda hapus, lalu pilih Delete (Hapus), dan konfirmasi penghapusan.

Perlindungan tingkat lanjut DNS Firewall

DNS Firewall Advanced mendeteksi kueri DNS yang mencurigakan berdasarkan tanda tangan ancaman yang diketahui dalam kueri DNS. Anda dapat menentukan jenis ancaman dalam aturan yang Anda gunakan dalam aturan DNS Firewall, yang terkait dengan Tampilan DNS.

DNS Firewall Advanced bekerja dengan mengidentifikasi tanda tangan ancaman DNS yang mencurigakan dengan memeriksa berbagai pengidentifikasi kunci dalam muatan DNS termasuk stempel waktu permintaan, frekuensi permintaan dan tanggapan, string kueri DNS, dan panjang, jenis atau ukuran kueri DNS keluar dan masuk. Berdasarkan jenis tanda tangan ancaman, Anda dapat mengonfigurasi kebijakan untuk memblokir, atau cukup log dan peringatan pada kueri. Dengan menggunakan serangkaian pengidentifikasi ancaman yang diperluas, Anda dapat melindungi terhadap ancaman DNS dari sumber domain yang mungkin belum diklasifikasikan oleh umpan intelijen ancaman yang dikelola oleh komunitas keamanan yang lebih luas.

Saat ini, DNS Firewall Advanced menawarkan perlindungan dari:

- Algoritma Pembuatan Domain () DGAs

DGAs digunakan oleh penyerang untuk menghasilkan sejumlah besar domain untuk meluncurkan serangan malware.

- Terowongan DNS

Tunneling DNS digunakan oleh penyerang untuk mengekstraksi data dari klien dengan menggunakan terowongan DNS tanpa membuat koneksi jaringan ke klien.

Untuk mempelajari cara membuat aturan, lihat [the section called “Konfigurasi dan kelola aturan DNS Firewall”](#).

Mengurangi skenario positif palsu

Jika Anda menghadapi skenario positif palsu dalam aturan yang menggunakan perlindungan DNS Firewall Advanced untuk memblokir kueri, lakukan langkah-langkah berikut:

1. Dalam log Global Resolver, identifikasi aturan dan perlindungan DNS Firewall Advanced yang menyebabkan false positive. Anda melakukan ini dengan menemukan log untuk kueri yang diblokir oleh DNS Firewall, tetapi yang ingin Anda izinkan. Catatan log mencantumkan Tampilan DNS, aturan, tindakan aturan, dan perlindungan DNS Firewall Advanced.
2. Buat aturan baru di Tampilan DNS yang secara eksplisit memungkinkan kueri yang diblokir. Saat Anda membuat aturan, Anda dapat menentukan daftar domain Anda sendiri hanya dengan spesifikasi domain yang ingin Anda izinkan. Ikuti panduan untuk manajemen aturan di [the section called “Konfigurasi dan kelola aturan DNS Firewall”](#).
3. Prioritaskan aturan baru di dalam aturan sehingga berjalan sebelum aturan yang menggunakan daftar terkelola. Untuk melakukan ini, berikan aturan baru pengaturan prioritas numerik yang lebih rendah.

Ketika Anda telah memperbarui aturan Anda, aturan baru akan secara eksplisit mengizinkan nama domain yang ingin Anda izinkan sebelum aturan pemblokiran berjalan.

Mengelola kebijakan keamanan DNS di Route 53 Global Resolver

Mengelola resolver global

Setelah membuat resolver global, Anda dapat melihat detailnya, mengedit konfigurasinya, dan mengelola sumber daya terkait dari halaman Global Resolvers.

Melihat detail resolver

Halaman Global Resolvers menampilkan daftar semua resolver Anda dengan informasi penting termasuk nama resolver, wilayah yang digunakan, tampilan DNS terkait, wilayah observabilitas, dan status operasional.

Mengedit resolver global

Anda dapat memodifikasi nama resolver dan deskripsi setelah pembuatan. Anda tidak dapat mengubah wilayah tempat resolver global diterapkan setelah pembuatan.

Mengelola aturan firewall

Setelah membuat aturan firewall, Anda dapat mengubah prioritas mereka, memperbarui konfigurasi mereka, atau menghapusnya sesuai kebutuhan.

Prioritas aturan dan urutan evaluasi

Aturan firewall dievaluasi dalam urutan prioritas, dengan angka yang lebih rendah diproses terlebih dahulu. Saat kueri cocok dengan beberapa aturan, hanya tindakan aturan pencocokan pertama yang diterapkan.

Memperbarui aturan firewall

Anda dapat memperbarui sebagian besar aspek aturan firewall setelah pembuatan, termasuk prioritas, tindakan, dan domain targetnya.

Mengkonfigurasi asosiasi zona host pribadi dengan Route 53 Global Resolver

Route 53 Global Resolver memungkinkan Anda menyelesaikan catatan yang terkait dengan zona host pribadi Route 53 dari klien resmi Anda. Anda dapat mengaitkan zona host pribadi Route 53 dengan tampilan DNS yang diizinkan untuk diselesaikan oleh klien Anda dengan tampilan DNS.

Topik

- [Kelola asosiasi zona yang dihosting pribadi dengan Route 53 Global Resolver](#)

Kelola asosiasi zona yang dihosting pribadi dengan Route 53 Global Resolver

Membuat zona host pribadi untuk aplikasi internal

Sebelum Anda dapat mengaitkan zona yang dihosting pribadi dengan tampilan DNS, Anda harus terlebih dahulu membuat zona menggunakan konsol Amazon Route 53 atau API.

Untuk membuat zona yang dihosting pribadi

1. Buka konsol Amazon Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih Buat zona yang di-hosting.
4. Untuk nama Domain, masukkan nama domain untuk zona pribadi Anda (misalnya, `internal.example.com`).
5. Untuk Jenis, pilih Zona yang dihosting pribadi.
6. VPCs Untuk mengasosiasikan dengan zona yang dihosting, pilih zona yang ingin VPCs Anda kaitkan dengan zona yang dihosting. Secara opsional, Anda dapat menggunakan operasi `CreateHostedZone` API untuk melewati memasukkan nilai karena Anda akan mengaitkan zona dengan Route 53 Global Resolver sebagai gantinya.
7. Pilih Buat zona yang di-hosting.

Setelah membuat zona host pribadi, tambahkan catatan DNS yang Anda butuhkan untuk layanan internal Anda.

Mengaitkan zona yang dihosting pribadi dengan tampilan DNS

Untuk mengaktifkan Route 53 Global Resolver untuk menyelesaikan kueri untuk zona host pribadi Anda, Anda harus mengaitkan zona tersebut dengan satu atau beberapa tampilan DNS.

Untuk mengaitkan zona yang dihosting pribadi dengan tampilan DNS

1. Di konsol Route 53 Global Resolver, navigasikan ke resolver global Anda.
2. Pilih tampilan DNS tempat Anda ingin mengaitkan zona host pribadi.
3. Di bagian Zona yang dihosting pribadi, pilih Zona yang dihosting asosiasikan.
4. Untuk zona Hosted, pilih zona host pribadi yang ingin Anda kaitkan.

5. Untuk nama Asosiasi, masukkan nama deskriptif untuk asosiasi ini.
6. Pilih zona yang dihosting Associate.

Proses asosiasi biasanya memakan waktu beberapa menit untuk diselesaikan. Setelah selesai, Route 53 Global Resolver akan menggunakan catatan di zona host pribadi untuk menjawab kueri DNS dari perangkat klien yang terkait dengan tampilan DNS.

Memantau aktivitas dan kinerja DNS dengan Route 53 Global Resolver

Route 53 Global Resolver menyediakan visibilitas komprehensif ke aktivitas DNS di seluruh organisasi Anda, memungkinkan Anda mengidentifikasi ancaman keamanan, menganalisis perilaku perangkat klien, dan mempertahankan kepatuhan. Bab ini mencakup alat pemantauan yang tersedia dan prosedur terperinci untuk menyiapkan pemantauan DNS, mengonfigurasi tujuan pencatatan, dan menganalisis data DNS untuk menyelidiki ancaman dan mengoptimalkan kinerja.

AWS menyediakan alat pemantauan ini untuk membantu Anda mempertahankan layanan DNS yang aman dan andal:

- Amazon CloudWatch melacak volume kueri DNS, waktu respons, dan peristiwa keamanan secara real time. Buat dasbor untuk memantau kinerja DNS di seluruh lokasi dan atur alarm untuk memberi tahu Anda saat volume kueri melonjak atau waktu respons meningkat yang Anda tentukan. Untuk Route 53 Global Resolver, Anda dapat memantau volume kueri, waktu respons, dan aktivitas pemfilteran. Untuk informasi selengkapnya, lihat [Panduan CloudWatch Pengguna Amazon](#).
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari EC2 instans Amazon CloudTrail, dan sumber lainnya. Route 53 Global Resolver dapat mengirimkan log kueri DNS langsung ke CloudWatch Log untuk pemantauan dan analisis waktu nyata. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon CloudWatch Logs](#).
- Amazon EventBridge dapat digunakan untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).

- AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS CloudTrail](#).

Topik

- [Dapatkan visibilitas ke aktivitas DNS dengan Route 53 Global Resolver](#)
- [Konfigurasi pemantauan dan pencatatan DNS dengan Route 53 Global Resolver](#)

Dapatkan visibilitas ke aktivitas DNS dengan Route 53 Global Resolver

Route 53 Global Resolver menyediakan kemampuan pencatatan kueri DNS yang komprehensif untuk memantau aktivitas perangkat klien dan mengidentifikasi ancaman keamanan. Aktifkan pencatatan kueri DNS di Route 53 Global Resolver untuk melihat situs web apa yang diakses perangkat klien, mengidentifikasi potensi ancaman keamanan, dan menganalisis pola resolusi DNS. Log menangkap informasi komprehensif tentang setiap kueri, termasuk kebijakan keamanan yang diterapkan.

Informasi apa yang ditangkap dalam log DNS

Setiap entri log kueri DNS memberikan informasi terperinci tentang aktivitas perangkat klien dan penegakan kebijakan keamanan:

- Informasi kueri - Nama domain, jenis kueri, kelas kueri, dan protokol yang digunakan
- Informasi perangkat klien - Alamat IP sumber, tampilan DNS, dan metode otentikasi
- Informasi respons - Kode respons, catatan jawaban, dan waktu respons
- Tindakan keamanan - Pencocokan aturan Firewall, hasil deteksi ancaman, dan tindakan yang diambil
- Metadata - Timestamp, ID penyelesaian global, Wilayah, dan informasi jejak

Format OCSF untuk integrasi keamanan

Log kueri DNS menggunakan Open Cybersecurity Schema Framework (OCSF), yang menyediakan format standar untuk data peristiwa keamanan. Format ini memungkinkan:

- Analisis standar - Skema yang konsisten di berbagai alat keamanan

- Peningkatan interoperabilitas - Integrasi mudah dengan SIEM dan platform analitik
- Korelasi yang ditingkatkan - Kemampuan untuk mengkorelasikan peristiwa DNS dengan data keamanan lainnya
- Kompatibilitas masa depan - Dukungan untuk persyaratan analisis keamanan yang terus berkembang

Contoh format log OCSF

Route 53 Global Resolver DNS log query mengikuti struktur skema OCSF, memberikan informasi rinci tentang setiap query DNS, respon, dan tindakan keamanan. Contoh berikut menunjukkan format log untuk kueri yang diizinkan dan ditolak.

Route 53 Global Resolver DNS log - Akses contoh yang diizinkan

Contoh ini menunjukkan kueri DNS yang diizinkan melalui aturan firewall. Log mencakup detail kueri, informasi respons, dan data pengayaan dengan pengidentifikasi khusus Route 53 Global Resolver.

```
{
  "action_id": 1,
  "action_name": "Allowed",
  "activity_id": 6,
  "activity_name": "Traffic",
  "category_name": "Network Activity",
  "category_uid": 4,
  "class_name": "DNS Activity",
  "class_uid": 4003,
  "cloud": {
    "provider": "AWS",
    "region": "us-east-1",
    "account": {
      "uid": "123456789012"
    }
  },
  "connection_info": {
    "direction": "Inbound",
    "direction_id": 1,
    "protocol_name": "udp",
    "protocol_num": 17,
    "protocol_ver": "",
    "uid": "db21d1739ddb423a"
  },
}
```

```
"duration": 1,
"end_time": 1761358379996,
"answers": [{
  "rdata": "3.3.3.3",
  "type": "A",
  "class": "IN",
  "ttl": 300
},
{
  "rdata": "3.3.3.4",
  "type": "A",
  "class": "IN",
  "ttl": 300
}],
"src_endpoint": {
  "ip": "3.3.3.1",
  "port": 56576
},
"enrichments": [{
  "name": "global-resolver",
  "value": "gr-a1b2c3d4fexample",
  "data": {
    "dns_view_id": "dnsv-a1b2c3d4fexample",
    "firewall_rule_id": "fr-a1b2c3d4fexample",
    "token_id": "t-a1b2c3d4fexample",
    "token_name": "device-123456",
    "token_expiration": "1789419206",
  }
}],
"message": "",
"metadata": {
  "version": "1.2.0",
  "product": {
    "name": "Global Resolver",
    "vendor_name": "AWS",
    "feature": {
      "name": "DNS"
    }
  }
},
"query": {
  "hostname": "example.com.",
  "class": "IN",
  "type": "A",
```

```

        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "NOERROR",
    "rcode_id": 0,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "start_time": 1761358379995,
    "status": "Success",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}

```

Route 53 Log DNS Resolver Global - Contoh akses ditolak

Contoh ini menunjukkan kueri DNS yang diblokir oleh aturan firewall. Log mencakup tindakan penolakan, larik jawaban kosong, dan kode respons REFUSED yang menunjukkan kueri tidak diproses.

```

{
    "action_id": 2,
    "action_name": "Denied",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
        "provider": "AWS",
        "region": "us-west-2",
        "account": {
            "uid": "123456789012"
        }
    }
},

```

```
"connection_info": {
  "direction": "Inbound",
  "direction_id": 1,
  "protocol_name": "tcp",
  "protocol_num": 6,
  "protocol_ver_id": 4,
  "uid": "9fdc6fbc09794d5e"
},
"duration": 1,
"end_time": 1761358379996,
"answers": [],
"src_endpoint": {
  "ip": "3.3.3.3",
  "port": 28276
},
"enrichments": [
  {
    "name": "global-resolver",
    "value": "gr-a1b2c3d4fexample",
    "data": {
      "dns_view_id": "dnsv-a1b2c3d4fexample",
      "firewall_rule_id": "fr-a1b2c3d4fexample",
      "token_id": "t-a1b2c3d4fexample",
      "token_name": "device-123456",
      "token_expiration": "1789419206",
    }
  }
],
"message": "",
"metadata": {
  "version": "1.2.0",
  "product": {
    "name": "Global Resolver",
    "vendor_name": "AWS",
    "feature": {
      "name": "DNS"
    }
  }
},
"query": {
  "hostname": "example.com.",
  "class": "IN",
  "type": "A",
  "opcode": "Query",
```



```
    "opcode_id": 0
  },
  "query_time": 1761358379995,
  "rcode": "REFUSED",
  "rcode_id": 5,
  "response_time": 1761358379995,
  "severity": "Informational",
  "severity_id": 1,
  "start_time": 1761358379995,
  "status": "Failure",
  "status_id": 1,
  "time": 1761358379995,
  "type_name": "DNS Activity: Traffic",
  "type_uid": 400306
}
```

Konfigurasi pemantauan dan pencatatan DNS dengan Route 53 Global Resolver

Konfigurasi pemantauan DNS di Route 53 Global Resolver untuk menangkap informasi terperinci tentang kueri, respons, dan tindakan keamanan DNS. Bagian ini mencakup langkah-langkah untuk mengatur tujuan pencatatan dan mengonfigurasi alat pemantauan.

Mengatur Wilayah observabilitas

Sebelum mengonfigurasi logging DNS, Anda harus menetapkan Wilayah observabilitas tempat log dan metrik akan disimpan. Wilayah ini menentukan di mana data pemantauan Anda diproses dan disimpan.

1. Buka konsol Route 53 Global Resolver di <https://console.aws.amazon.com/route53globalresolver/>
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di bagian wilayah Observabilitas, pilih Setel wilayah.
4. Pilih AWS Wilayah tempat Anda ingin menyimpan data pemantauan, lalu pilih Setel wilayah.

Setelah menyetel wilayah observabilitas, Anda dapat mengonfigurasi tujuan pengiriman log di wilayah tersebut.

Memecahkan masalah DNS dengan Route 53 Global Resolver

Route 53 Global Resolver menyediakan kemampuan resolusi DNS yang komprehensif, tetapi terkadang Anda mungkin perlu memecahkan masalah konektivitas, kinerja, atau konfigurasi. Gunakan log DNS, data pemantauan, dan teknik diagnostik untuk mengidentifikasi dan menyelesaikan masalah yang memengaruhi resolusi DNS perangkat klien dengan Route 53 Global Resolver. Bab ini memberikan pendekatan sistematis untuk memecahkan masalah DNS umum dan mengoptimalkan kinerja.

Topik

- [Mendiagnosis masalah konektivitas DNS dengan Route 53 Global Resolver](#)
- [Mengatasi masalah kinerja DNS dengan Route 53 Global Resolver](#)
- [Memecahkan masalah konfigurasi di Route 53 Global Resolver](#)
- [Memecahkan masalah akses sumber daya internal](#)

Mendiagnosis masalah konektivitas DNS dengan Route 53 Global Resolver

Route 53 Global Resolver menyediakan resolusi DNS yang andal, tetapi masalah konektivitas kadang-kadang dapat terjadi karena konfigurasi, otentikasi, atau masalah jaringan. Ketika perangkat klien tidak dapat menyelesaikan nama domain menggunakan Route 53 Global Resolver, gunakan pendekatan sistematis ini untuk mengidentifikasi dan menyelesaikan masalah konektivitas.

Perangkat klien tidak dapat menyelesaikan domain

Ikuti langkah-langkah berikut untuk mendiagnosis kegagalan resolusi:

1. Verifikasi kueri mencapai resolver global
 - Periksa log kueri DNS untuk kueri dari alamat IP perangkat klien yang terpengaruh
 - Konfirmasikan perangkat klien dikonfigurasi dengan alamat IP anycast yang benar
 - Uji konektivitas jaringan dari perangkat klien ke anycast IPs
2. Periksa otentikasi perangkat klien
 - Verifikasi perangkat klien diautentikasi ke tampilan DNS yang benar
 - Periksa aturan Sumber Akses untuk alamat IP perangkat klien atau blok CIDR
 - Konfirmasi token akses valid dan tidak kedaluwarsa (untuk otentikasi berbasis token)
3. Tinjau aturan firewall

- Periksa apakah aturan firewall memblokir kueri
- Tinjau prioritas aturan dan pastikan aturan izin memiliki prioritas lebih tinggi daripada aturan blok
- Verifikasi pengaturan perilaku gagal buka firewall

4. Konfirmasikan asosiasi tampilan DNS

- Verifikasi asosiasi zona yang dihosting pribadi untuk domain internal
- Periksa apakah catatan DNS ada di zona host pribadi terkait
- Pastikan nama domain dalam kueri sama persis dengan nama zona

Kegagalan resolusi intermiten

Untuk masalah resolusi DNS sporadis, selidiki penyebab potensial ini:

Masalah otentikasi

- Periksa pola kedaluwarsa dan pembaruan token akses
- Tinjau log otentikasi untuk upaya otentikasi yang gagal
- Verifikasi sinkronisasi jam perangkat klien untuk validasi token

Konektivitas jaringan

- Memantau perubahan jalur jaringan atau masalah perutean
- Periksa perubahan konfigurasi perangkat firewall atau NAT
- Verifikasi perutean anycast yang konsisten ke Wilayah terdekat

Kondisi layanan

- Periksa AWS Service Health Dashboard untuk masalah Route 53 Global Resolver
- Tinjau CloudWatch metrik untuk lonjakan tingkat kesalahan
- Pantau status asosiasi zona yang dihosting pribadi

Resolusi publik yang tidak terduga

Saat kueri diselesaikan ke DNS publik, bukan zona yang dihosting pribadi:

1. Verifikasi konfigurasi zona yang dihosting pribadi

- Konfirmasikan zona yang dihosting pribadi berisi catatan DNS yang diharapkan
- Periksa apakah nama rekaman sama persis dengan domain yang ditanyakan

- Verifikasi jenis rekaman cocok dengan jenis kueri (A, AAAA, CNAME, dll.)
2. Periksa asosiasi tampilan DNS
 - Verifikasi bahwa zona yang dihosting pribadi dikaitkan dengan tampilan DNS yang benar
 - Konfirmasikan perangkat klien diautentikasi ke tampilan DNS
 - Periksa status asosiasi di konsol
 3. Tinjau aturan firewall
 - Periksa aturan firewall yang mungkin memblokir kueri zona pribadi
 - Verifikasi urutan evaluasi aturan dan prioritas
 - Tinjau log kueri DNS untuk tindakan firewall

Mengatasi masalah kinerja DNS dengan Route 53 Global Resolver

Route 53 Global Resolver dirancang untuk kinerja optimal dengan arsitektur anycast global, tetapi berbagai faktor dapat mempengaruhi kecepatan resolusi DNS. Atasi resolusi DNS yang lambat dan optimalkan waktu respons kueri untuk kinerja perangkat klien yang lebih baik menggunakan Route 53 Global Resolver.

Resolusi DNS lambat

Untuk mendiagnosis dan mengatasi waktu respons DNS yang lambat:

1. Menganalisis waktu respons kueri
 - Gunakan log kueri DNS untuk mengidentifikasi kueri dengan waktu respons tinggi
 - Bandingkan waktu respons di berbagai domain dan jenis kueri
 - Pantau tren waktu respons dari waktu ke waktu
2. Periksa volume kueri yang tinggi
 - Pantau CloudWatch metrik untuk lonjakan volume kueri
 - Identifikasi perangkat klien atau tampilan DNS yang menghasilkan kueri berlebihan
 - Cari pola kueri yang mungkin menunjukkan kesalahan konfigurasi
3. Tinjau kinerja cache
 - Analisis tingkat hit cache untuk domain yang sering ditanyakan
 - Tinjau pengaturan TTL untuk catatan DNS
 - Pertimbangkan untuk menyesuaikan nilai TTL berdasarkan pola kueri

4. Verifikasi pemilihan Wilayah yang optimal

- Pastikan wilayah resolver global dekat dengan lokasi perangkat klien
- Pantau perutean anycast untuk mengonfirmasi kueri mencapai Wilayah terdekat
- Pertimbangkan untuk menambahkan wilayah jika perangkat klien secara geografis jauh

Strategi pengoptimalan kinerja

Gunakan strategi ini untuk mengoptimalkan kinerja DNS:

Pengoptimalan cache

- Sesuaikan nilai TTL berdasarkan pola kueri dan ubah frekuensi
- Gunakan lebih lama TTLs untuk catatan stabil, lebih pendek TTLs untuk catatan yang sering berubah
- Pantau tingkat hit cache dan TTLs sesuaikan

Optimalisasi wilayah

- Terapkan resolver global di wilayah yang paling dekat dengan konsentrasi perangkat klien
- Pantau pola perutean kueri dan waktu respons berdasarkan wilayah
- Pertimbangkan untuk menambahkan wilayah untuk cakupan geografis yang lebih baik

Optimalisasi protokol

- Pilih protokol DNS yang sesuai berdasarkan persyaratan keamanan dan kinerja
- Pertimbangkan DNS-over-HTTPS (DoH) untuk koneksi terenkripsi dengan manfaat caching
- Gunakan DNS-over-TLS (DoT) untuk koneksi terenkripsi dengan overhead yang lebih rendah

Pengoptimalan aturan

- Tinjau dan optimalkan prioritas dan kompleksitas aturan firewall
- Tempatkan aturan yang sering dicocokkan lebih tinggi dalam urutan prioritas
- Sederhanakan kondisi aturan yang kompleks jika memungkinkan

Memecahkan masalah konfigurasi di Route 53 Global Resolver

Route 53 Global Resolver menawarkan opsi konfigurasi ekstensif untuk tampilan DNS, otentikasi, dan aturan firewall, yang terkadang dapat menyebabkan konflik konfigurasi atau ketidakcocokan. Identifikasi dan selesaikan masalah konfigurasi Route 53 Global Resolver umum yang memengaruhi resolusi DNS.

Masalah otentikasi

Masalah otentikasi umum dan solusi:

Ketidakcocokan aturan Sumber Akses

- Verifikasi alamat IP perangkat klien cocok dengan blok CIDR yang dikonfigurasi
- Periksa NAT atau perangkat proxy yang mengubah alamat IP sumber
- Pastikan aturan Sumber Akses mencakup semua rentang IP perangkat klien yang diharapkan

Kegagalan otentikasi token

- Verifikasi token dikonfigurasi dengan benar pada perangkat klien
- Periksa tanggal kedaluwarsa token dan proses perpanjangan
- Pastikan jam perangkat klien disinkronkan untuk validasi token

Ketidakcocokan protokol

- Verifikasi perangkat klien menggunakan protokol yang diizinkan oleh aturan Access Source
- Periksa apakah konfigurasi DoH dan DoT cocok dengan protokol token
- Pastikan aturan firewall tidak memblokir protokol yang diperlukan

Masalah konfigurasi tampilan DNS

Masalah konfigurasi tampilan DNS umum:

Asosiasi tampilan DNS salah

- Verifikasi perangkat klien diautentikasi ke tampilan DNS yang dimaksud
- Periksa apakah zona yang dihosting pribadi dikaitkan dengan tampilan DNS yang benar
- Tinjau aturan firewall yang diterapkan pada setiap tampilan DNS

Konflik pengaturan DNS

- Tinjau pengaturan validasi DNSSEC untuk kompatibilitas dengan perangkat klien
- Periksa pengaturan EDNS Client Subnet untuk privasi dan keseimbangan kinerja
- Verifikasi perilaku fail-open firewall selaras dengan persyaratan keamanan

Masalah aturan firewall

Masalah konfigurasi aturan firewall umum:

Konflik prioritas aturan

- Tinjau urutan evaluasi aturan dan pastikan penugasan prioritas yang benar
- Periksa aturan blok dengan prioritas lebih tinggi dari aturan izin yang dimaksudkan
- Perubahan aturan pengujian di lingkungan yang terkendali sebelum penerapan produksi

Ketidakcocokan daftar domain

- Verifikasi spesifikasi domain dalam daftar domain khusus
- Periksa pola wildcard untuk sintaks dan cakupan yang benar
- Pastikan daftar domain diperbarui dan disinkronkan

Memecahkan masalah akses sumber daya internal

Masalah dan solusi umum saat mengelola akses sumber daya internal:

Perangkat klien tidak menyelesaikan catatan zona pribadi

- Verifikasi bahwa zona yang dihosting pribadi dikaitkan dengan tampilan DNS yang benar
- Periksa apakah perangkat klien diautentikasi ke tampilan DNS yang benar
- Pastikan nama domain dalam kueri sama persis dengan nama zona
- Verifikasi catatan DNS yang ada di zona host pribadi

Kegagalan resolusi intermiten

- Periksa status asosiasi di konsol
- Tinjau log kueri DNS untuk pola kesalahan
- Verifikasi konektivitas jaringan antara Route 53 Global Resolver dan Amazon Route 53

Resolusi publik yang tidak terduga

- Konfirmasikan zona yang dihosting pribadi berisi catatan yang diharapkan
- Periksa aturan firewall yang mungkin memblokir kueri
- Verifikasi kueri berasal dari perangkat klien yang terkait dengan tampilan DNS

Kuota untuk Route 53 Global Resolver

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

[Untuk melihat kuota untuk Route 53 Global Resolver, buka konsol Service Quotas.](#) Di panel navigasi, pilih AWS layanan dan pilih Route 53 Global Resolver.

Untuk meminta peningkatan kuota, lihat [Meminta Peningkatan Kuota](#) dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan [formulir penambahan batas](#).

AWS Akun Anda memiliki kuota berikut yang terkait dengan Route 53 Global Resolver.

Kuota lembut

Tabel berikut menjelaskan kuota di Route 53 Global Resolver yang dapat ditingkatkan. Untuk informasi tentang mengubah kuota, lihat [Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas](#).

Untuk beberapa pelanggan, kuota akun Anda mungkin di bawah kuota yang dipublikasikan ini. Jika Anda merasa salah menemukan kesalahan batas Sumber Daya melebihi, gunakan [konsol Service Quotas untuk meminta peningkatan kuota](#).

Sumber daya	Kuota bawaan	Dapat Disesuaikan
Penyelesai global per akun	2	Ya
Tampilan DNS per penyelesai global	5	Ya
Tampilan DNS per akun	50	Ya
Daftar domain per akun	1.000	Ya
Domain per daftar domain	100.000	Ya
Domain dalam file yang diimpor dari S3	10.000	Ya
Jumlah domain di semua Aturan Firewall	1.000.000	Ya
Aturan firewall per tampilan DNS	100	Ya

Sumber daya	Kuota bawaan	Dapat Disesuaikan
Akses token per penyelesaian global	5.000	Ya
Sumber Akses per penyelesaian global	1.000	Ya
Sumber Akses ukuran CIDR per resolver global	65.000	Tidak
Zona yang dihosting pribadi per tampilan DNS	1.000	Ya

Kuota keras

Tabel berikut menjelaskan kuota di Route 53 Global Resolver yang tidak dapat ditingkatkan.

Sumber daya atau operasi	Kuota
Konfigurasi pengiriman log per (penyelesai global, tipe tujuan, Wilayah)	1

Membuat sumber daya Amazon Route 53 dan Route 53 VPC Resolver dengan AWS CloudFormation

Amazon Route 53 dan Route 53 VPC Resolver terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan menyiapkan AWS sumber daya sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan, dan menyediakan serta CloudFormation mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakan CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya Route 53 dan VPC Resolver Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

Route 53, VPC Resolver, dan template CloudFormation

[Untuk menyediakan dan mengonfigurasi sumber daya untuk Route 53, VPC Resolver, dan layanan terkait, Anda harus memahami templat.CloudFormation](#) Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan JSON atau YAMAL, Anda dapat menggunakan CloudFormation Designer untuk membantu Anda memulai dengan template. CloudFormation Untuk informasi lebih lanjut, lihat [Apa itu CloudFormation Designer?](#) dalam AWS CloudFormation User Guide.

Route 53 mendukung pembuatan jenis sumber daya berikut di CloudFormation:

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Untuk informasi selengkapnya, termasuk contoh templat JSON dan YAMAL untuk sumber daya Route 53, lihat [referensi jenis sumber daya Amazon Route 53](#) di AWS CloudFormation Panduan Pengguna.

VPC Resolver mendukung pembuatan jenis sumber daya berikut di: CloudFormation

- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallRuleGroupAssociation`
- `AWS::Route53Resolver::ResolverDNSSECConfig`
- `AWS::Route53Resolver::ResolverEndpoint`
- `AWS::Route53Resolver::ResolverQueryLoggingConfig`
- `AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`
- `AWS::Route53Resolver::ResolverRule`
- `AWS::Route53Resolver::ResolverRuleAssociation`

Untuk informasi selengkapnya, termasuk contoh template JSON dan YAMAL untuk sumber daya VPC Resolver, lihat referensi tipe sumber daya Route [53 VPC Resolver](#) di Panduan Pengguna.AWS CloudFormation

Praktik terbaik untuk Rute 53 dan CloudFormation

Saat menggunakan CloudFormation untuk mengelola sumber daya Route 53, ikuti praktik terbaik ini untuk menghindari masalah umum dan memastikan penerapan yang andal.

Memahami konsistensi akhirnya

Route 53 menggunakan model yang pada akhirnya konsisten untuk perubahan DNS. Hal ini dapat mempengaruhi CloudFormation operasi, terutama selama rollback dan perubahan berturut-turut yang cepat.

Important

Ketika CloudFormation upaya untuk memutar kembali catatan DNS berubah, rollback mungkin gagal karena model konsistensi Route 53 akhirnya. Jika CloudFormation mencoba membuat ulang catatan yang baru saja dihapus tetapi tampaknya masih ada karena

konsistensi akhirnya, Anda mungkin menemukan `InvalidChangeBatch` kesalahan yang membuat DNS Anda dalam keadaan rusak.

Untuk meminimalkan masalah yang terkait dengan konsistensi akhirnya:

- Rencanakan perubahan dengan hati-hati - Hindari membuat perubahan berturut-turut yang cepat pada catatan DNS yang sama
- Uji di non-produksi terlebih dahulu - Selalu uji perubahan DNS di lingkungan pengembangan sebelum diterapkan ke produksi
- Pantau penerapan - Tonton peristiwa CloudFormation tumpukan secara dekat selama penerapan terkait DNS. Untuk panduan pemantauan, lihat [Memantau Amazon Route 53](#).
- Siapkan prosedur rollback - Siapkan prosedur pemulihan manual jika rollback otomatis gagal

Pengurutan catatan DNS dan logis IDs

Saat membuat beberapa catatan DNS CloudFormation, berhati-hatilah dengan urutan catatan dan penetapan ID logis.

Warning

Jika Anda mendefinisikan catatan DNS dalam array atau daftar dalam CloudFormation template Anda, memasukkan catatan baru di tengah daftar dapat menyebabkan CloudFormation untuk menetapkan kembali logis IDs ke catatan yang ada. Ini memicu penggantian rekaman yang dapat menyebabkan gangguan layanan dan kegagalan rollback.

Praktik terbaik untuk manajemen catatan DNS:

- Gunakan logis eksplisit IDs - Selalu tetapkan logis eksplisit dan bermakna IDs ke catatan DNS daripada mengandalkan indeks array. Untuk informasi selengkapnya tentang CloudFormation logika IDs, lihat [struktur bagian Sumber daya](#) di Panduan AWS CloudFormation Pengguna
- Tambahkan catatan baru - Saat menambahkan catatan DNS baru ke daftar yang ada, tambahkan ke akhir daripada memasukkannya di tengah
- Catatan terkait kelompok - Pertimbangkan `AWS::Route53::RecordSetGroup` untuk menggunakan untuk mengelola catatan terkait bersama-sama. Untuk informasi selengkapnya, lihat [AWS::Route53::RecordSetKelompokkan](#) di Panduan AWS CloudFormation Pengguna.

- Tinjau set perubahan - Selalu tinjau set CloudFormation perubahan sebelum penerapan untuk mengidentifikasi penggantian rekaman yang tidak terduga. Untuk informasi selengkapnya, lihat [Memperbarui tumpukan menggunakan set perubahan](#) di Panduan AWS CloudFormation Pengguna.

Menangani kegagalan rollback

Jika CloudFormation rollback gagal karena masalah terkait DNS, Anda mungkin perlu melakukan pemulihan manual.

Untuk melakukan pemulihan manual dari rollback DNS yang gagal

1. Identifikasi catatan DNS yang gagal dengan meninjau peristiwa CloudFormation tumpukan dan catatan zona yang dihosting Route 53
2. Buat atau perbarui catatan DNS yang hilang secara manual melalui konsol atau API Route 53. Untuk informasi tentang membuat catatan, lihat [Bekerja dengan catatan](#).
3. Setelah DNS dipulihkan, perbarui CloudFormation template Anda agar sesuai dengan status saat ini
4. Terapkan templat yang dikoreksi untuk menyinkronkan CloudFormation kembali dengan sumber daya yang sebenarnya

Untuk mencegah kegagalan rollback:

- Hindari membuat perubahan yang dapat memicu penggantian catatan DNS selama periode lalu lintas tinggi
- Menerapkan pemeriksaan dan pemantauan kesehatan untuk mendeteksi masalah DNS dengan cepat. Untuk informasi tentang pemeriksaan kesehatan, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).
- Pertimbangkan untuk menggunakan strategi penyebaran biru-hijau untuk perubahan DNS kritis. Untuk informasi selengkapnya tentang praktik terbaik penerapan, lihat [Praktik terbaik untuk Amazon Route 53](#).
- Dokumen prosedur darurat untuk pemulihan DNS manual

Pelajari lebih lanjut tentang CloudFormation

Untuk mempelajari selengkapnya CloudFormation, lihat sumber daya berikut:

- [AWS CloudFormation](#)
- [AWS CloudFormation Panduan Pengguna](#)
- [CloudFormation Referensi API](#)
- [AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah](#)

Contoh kode untuk Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan Route 53 dengan kit pengembangan AWS perangkat lunak (SDK).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh kode

- [Contoh kode untuk Route 53 menggunakan AWS SDKs](#)
 - [Contoh dasar untuk Route 53 menggunakan AWS SDKs](#)
 - [Tindakan untuk Route 53 menggunakan AWS SDKs](#)
 - [Gunakan ChangeResourceRecordSets dengan CLI](#)
 - [Gunakan CreateHostedZone dengan CLI](#)
 - [Gunakan DeleteHostedZone dengan CLI](#)
 - [Gunakan GetHostedZone dengan CLI](#)
 - [Gunakan ListHostedZones dengan AWS SDK atau CLI](#)
 - [Gunakan ListHostedZonesByName dengan CLI](#)
 - [Gunakan ListQueryLoggingConfigs dengan CLI](#)
 - [Contoh kode untuk pendaftaran domain Route 53 menggunakan AWS SDKs](#)
 - [Contoh dasar untuk pendaftaran domain Route 53 menggunakan AWS SDKs](#)
 - [Hello Route 53 pendaftaran domain](#)
 - [Pelajari dasar-dasar pendaftaran domain Route 53 dengan AWS SDK](#)
 - [Tindakan untuk pendaftaran domain Route 53 menggunakan AWS SDKs](#)
 - [Gunakan CheckDomainAvailability dengan AWS SDK atau CLI](#)
 - [Gunakan CheckDomainTransferability dengan AWS SDK atau CLI](#)
 - [Gunakan GetDomainDetail dengan AWS SDK atau CLI](#)
 - [Gunakan GetDomainSuggestions dengan AWS SDK atau CLI](#)
 - [Gunakan GetOperationDetail dengan AWS SDK atau CLI](#)
 - [Gunakan ListDomains dengan AWS SDK atau CLI](#)
 - [Gunakan ListOperations dengan AWS SDK atau CLI](#)

- [Gunakan ListPrices dengan AWS SDK](#)
- [Gunakan RegisterDomain dengan AWS SDK atau CLI](#)
- [Gunakan ViewBilling dengan AWS SDK atau CLI](#)

Contoh kode untuk Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan Route 53 dengan kit pengembangan AWS perangkat lunak (SDK).

Tindakan merupakan kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Sementara tindakan menunjukkan cara memanggil fungsi layanan individual, Anda dapat melihat tindakan dalam konteks dalam skenario terkait.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh kode

- [Contoh dasar untuk Route 53 menggunakan AWS SDKs](#)
 - [Tindakan untuk Route 53 menggunakan AWS SDKs](#)
 - [Gunakan ChangeResourceRecordSets dengan CLI](#)
 - [Gunakan CreateHostedZone dengan CLI](#)
 - [Gunakan DeleteHostedZone dengan CLI](#)
 - [Gunakan GetHostedZone dengan CLI](#)
 - [Gunakan ListHostedZones dengan AWS SDK atau CLI](#)
 - [Gunakan ListHostedZonesByName dengan CLI](#)
 - [Gunakan ListQueryLoggingConfigs dengan CLI](#)

Contoh dasar untuk Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan dasar-dasar Amazon Route 53 dengan AWS SDKs.

Contoh

- [Tindakan untuk Route 53 menggunakan AWS SDKs](#)

- [Gunakan ChangeResourceRecordSets dengan CLI](#)
- [Gunakan CreateHostedZone dengan CLI](#)
- [Gunakan DeleteHostedZone dengan CLI](#)
- [Gunakan GetHostedZone dengan CLI](#)
- [Gunakan ListHostedZones dengan AWS SDK atau CLI](#)
- [Gunakan ListHostedZonesByName dengan CLI](#)
- [Gunakan ListQueryLoggingConfigs dengan CLI](#)

Tindakan untuk Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara melakukan tindakan Route 53 individual dengan AWS SDKs. Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan instruksi untuk mengatur dan menjalankan kode.

Contoh berikut hanya mencakup tindakan yang paling umum digunakan. Untuk daftar lengkapnya, lihat [Referensi API Amazon Route 53](#).

Contoh

- [Gunakan ChangeResourceRecordSets dengan CLI](#)
- [Gunakan CreateHostedZone dengan CLI](#)
- [Gunakan DeleteHostedZone dengan CLI](#)
- [Gunakan GetHostedZone dengan CLI](#)
- [Gunakan ListHostedZones dengan AWS SDK atau CLI](#)
- [Gunakan ListHostedZonesByName dengan CLI](#)
- [Gunakan ListQueryLoggingConfigs dengan CLI](#)

Gunakan **ChangeResourceRecordSets** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan `ChangeResourceRecordSets`.

CLI

AWS CLI

Untuk membuat, memperbarui, atau menghapus kumpulan catatan sumber daya

change-resource-record-sets Perintah berikut membuat catatan sumber daya yang ditetapkan menggunakan hosted-zone-id Z1R8UBAEXAMPLE dan konfigurasi berformat JSON dalam file: C:\awscli\route53\change-resource-record-sets.json

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Untuk informasi selengkapnya, lihat POST ChangeResourceRecordSets di Referensi API Amazon Route 53.

Konfigurasi dalam file JSON tergantung pada jenis kumpulan catatan sumber daya yang ingin Anda buat:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Sintaks dasar:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

Sintaks tertimbang:

```
{
  "Comment": "optional comment about the changes in this change batch request",
```

```

"Changes": [
  {
    "Action": "CREATE"|"DELETE"|"UPSERT",
    "ResourceRecordSet": {
      "Name": "DNS domain name",
      "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
      "SetIdentifier": "unique description for this resource record set",
      "Weight": value between 0 and 255,
      "TTL": time to live in seconds,
      "ResourceRecords": [
        {
          "Value": "applicable value for the record type"
        },
        {...}
      ],
      "HealthCheckId": "optional ID of an Amazon Route 53 health check"
    }
  },
  {...}
]
}

```

Sintaks Alias:

```

{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
bucket, Elastic Load Balancing load balancer, or another resource record set in
this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    }
  ]
}

```

```

    },
    {...}
  ]
}

```

Sintaks Alias Tertimbang:

```

{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
bucket, Elastic Load Balancing load balancer, or another resource record set in
this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}

```

Sintaks Latensi:

```

{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",

```

```

    "SetIdentifier": "unique description for this resource record set",
    "Region": "Amazon EC2 region name",
    "TTL": time to live in seconds,
    "ResourceRecords": [
      {
        "Value": "applicable value for the record type"
      },
      {...}
    ],
    "HealthCheckId": "optional ID of an Amazon Route 53 health check"
  }
},
{...}
]
}

```

Sintaks Alias Latensi:

```

{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
bucket, Elastic Load Balancing load balancer, or another resource record set in
this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}

```

Sintaks Failover:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaks Alias Failover:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
hosted zone",

```

```

        "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
        bucket, Elastic Load Balancing load balancer, or another resource record set in
        this hosted zone",
        "EvaluateTargetHealth": true|false
    },
    "HealthCheckId": "optional ID of an Amazon Route 53 health check"
}
},
{...}
]
}

```

- Untuk detail API, lihat [ChangeResourceRecordSets](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini membuat catatan A untuk `www.example.com` dan mengubah catatan A untuk `test.example.com` dari `192.0.2.3` menjadi `192.0.2.1`. Perhatikan bahwa nilai untuk perubahan catatan tipe TXT harus dalam tanda kutip ganda. Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan `Get-R53Change` cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"

```

```

$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
    and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
    ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params

```

Contoh 2: Contoh ini menunjukkan cara membuat kumpulan catatan sumber daya alias. 'Z222222222' adalah ID dari zona yang dihosting Amazon Route 53 tempat Anda membuat kumpulan catatan sumber daya alias. 'example.com' adalah puncak zona tempat Anda ingin membuat alias dan 'www.example.com' adalah subdomain yang Anda juga ingin membuat alias. 'Z11111111111' adalah contoh ID zona yang dihosting untuk penyeimbang beban dan 'example-load-balancer-1111111111.us-east-1.elb.amazonaws.com' adalah contoh nama domain penyeimbang beban yang digunakan Amazon Route 53 untuk menanggapi kueri untuk example.com dan www.example.com. Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan Get-R53Change cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"

```



```

$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z2222222222"
    ChangeBatch_Comment="This change batch creates two alias resource record sets,
    one for the zone apex, example.com, and one for www.example.com, that both point
    to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Contoh 3: Contoh ini membuat dua catatan A untuk `www.example.com`. Seperempat dari waktu ($1/(1+3)$), Amazon Route 53 menanggapi kueri untuk `www.example.com` dengan dua nilai untuk kumpulan catatan sumber daya pertama (192.0.2.9 dan 192.0.2.10). Tiga perempat waktu ($3/(1+3)$) Amazon Route 53 menanggapi kueri untuk `www.example.com` dengan dua nilai untuk kumpulan catatan sumber daya kedua (192.0.2.11 dan 192.0.2.12). Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan `Get-R53Change` cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"

```

```

$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
    each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Contoh 4: Contoh ini menunjukkan cara membuat kumpulan catatan sumber daya alias tertimbang dengan asumsi bahwa example.com adalah domain yang ingin Anda buat kumpulan catatan sumber daya alias tertimbang. SetIdentifier membedakan dua set catatan sumber daya alias tertimbang satu sama lain. Elemen ini diperlukan karena elemen Nama dan Jenis memiliki nilai yang sama untuk kedua kumpulan catatan sumber daya. Z11111111111111 dan Z3333333333333333 adalah contoh zona host untuk penyeimbang beban ELB yang ditentukan oleh nilai. IDs DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com dan example-load-balancer-4444444444.us-east-1.elb.amazonaws.com adalah contoh domain Elastic Load Balancing dari mana Amazon Route 53 menanggapi kueri untuk example.com. Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan Get-R53Change cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z11111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

```

```

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z555555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
    record sets. Amazon Route 53 responds to queries for example.com with the first
    ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Contoh 5: Contoh ini membuat dua set catatan sumber daya alias latensi, satu untuk penyeimbang beban ELB di wilayah AS Barat (Oregon) (us-west-2), dan satu lagi untuk penyeimbang beban di wilayah Asia Pasifik (Singapura) (ap-southeast-1). Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan Get-R53Change cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"

```

```

$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
    record sets, one for the US West (Oregon) region and one for the Asia Pacific
    (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

- Untuk detail API, lihat [ChangeResourceRecordSets](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini membuat catatan A untuk `www.example.com` dan mengubah catatan A untuk `test.example.com` dari `192.0.2.3` menjadi `192.0.2.1`. Perhatikan bahwa nilai untuk perubahan catatan tipe TXT harus dalam tanda kutip ganda. Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan `Get-R53Change` cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```

$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600

```

```

$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords = @()
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
    and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
    ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params

```

Contoh 2: Contoh ini menunjukkan cara membuat kumpulan catatan sumber daya alias. 'Z222222222' adalah ID dari zona yang dihosting Amazon Route 53 tempat Anda membuat kumpulan catatan sumber daya alias. 'example.com' adalah puncak zona tempat Anda ingin membuat alias dan 'www.example.com' adalah subdomain yang Anda juga ingin membuat alias. 'Z11111111111' adalah contoh ID zona yang dihosting untuk penyeimbang beban dan 'example-load-balancer-1111111111.us-east-1.elb.amazonaws.com' adalah contoh nama domain penyeimbang beban yang digunakan Amazon Route 53 untuk menanggapi kueri untuk example.com dan www.example.com. Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan Get-R53Change cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```
$change1 = New-Object Amazon.Route53.Model.Change
```

```

$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z2222222222"
    ChangeBatch_Comment="This change batch creates two alias resource record sets,
    one for the zone apex, example.com, and one for www.example.com, that both point
    to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Contoh 3: Contoh ini membuat dua catatan A untuk `www.example.com`. Seperempat dari waktu ($1/(1+3)$), Amazon Route 53 menanggapi kueri untuk `www.example.com` dengan dua nilai untuk kumpulan catatan sumber daya pertama (`192.0.2.9` dan `192.0.2.10`). Tiga perempat waktu ($3/(1+3)$) Amazon Route 53 menanggapi kueri untuk `www.example.com` dengan dua nilai untuk kumpulan catatan sumber daya kedua (`192.0.2.11` dan `192.0.2.12`). Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan `Get-R53Change` cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```
$change1 = New-Object Amazon.Route53.Model.Change
```

```

$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
    each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params

```

Contoh 4: Contoh ini menunjukkan cara membuat kumpulan catatan sumber daya alias tertimbang dengan asumsi bahwa example.com adalah domain yang ingin Anda buat kumpulan catatan sumber daya alias tertimbang. SetIdentifier membedakan dua set catatan sumber daya alias tertimbang satu sama lain. Elemen ini diperlukan karena elemen Nama dan Jenis memiliki nilai yang sama untuk kedua kumpulan catatan sumber daya. Z11111111111111 dan Z33333333333333 adalah contoh zona host untuk penyeimbang beban ELB yang ditentukan oleh nilai. IDs DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com dan example-load-balancer-4444444444.us-east-1.elb.amazonaws.com adalah contoh domain Elastic Load Balancing dari mana Amazon Route 53 menanggapi kueri untuk example.com. Lihat dokumentasi

Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan Get-R53Change cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z11111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z33333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
    record sets. Amazon Route 53 responds to queries for example.com with the first
    ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Contoh 5: Contoh ini membuat dua set catatan sumber daya alias latensi, satu untuk penyeimbang beban ELB di wilayah AS Barat (Oregon) (us-west-2), dan satu lagi untuk

penyeimbang beban di wilayah Asia Pasifik (Singapura) (ap-southeast-1). Lihat dokumentasi Amazon Route 53 untuk detail selengkapnya. Anda dapat menggunakan Get-R53Change cmdlet untuk melakukan polling untuk menentukan kapan perubahan selesai.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z11111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
    Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z22222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z555555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
record sets, one for the US West (Oregon) region and one for the Asia Pacific
(Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- Untuk detail API, lihat [ChangeResourceRecordSets](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **CreateHostedZone** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan `CreateHostedZone`.

CLI

AWS CLI

Untuk membuat zona yang dihosting

`create-hosted-zone` Perintah berikut menambahkan zona host bernama `example.com` menggunakan referensi `2014-04-01-18:47` pemanggil. Komentar opsional mencakup spasi, sehingga harus dilampirkan dalam tanda kutip:

```
aws route53 create-hosted-zone --name example.com --caller-  
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Untuk informasi selengkapnya, lihat Bekerja dengan Zona yang Dihosting di Panduan Pengembang Amazon Route 53.

- Untuk detail API, lihat [CreateHostedZone](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Membuat zona host baru bernama 'example.com', terkait dengan kumpulan delegasi yang dapat digunakan kembali. Perhatikan bahwa Anda harus memberikan nilai untuk `CallerReference` parameter sehingga permintaan yang perlu dicoba lagi jika perlu tanpa risiko mengeksekusi operasi dua kali. Karena zona yang dihosting sedang dibuat di VPC, zona ini secara otomatis bersifat pribadi dan Anda tidak boleh mengatur parameter `-HostedZoneConfig_PrivateZone`.

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- Untuk detail API, lihat [CreateHostedZone](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Membuat zona host baru bernama 'example.com', terkait dengan kumpulan delegasi yang dapat digunakan kembali. Perhatikan bahwa Anda harus memberikan nilai untuk CallerReference parameter sehingga permintaan yang perlu dicoba lagi jika perlu tanpa risiko mengeksekusi operasi dua kali. Karena zona yang dihosting sedang dibuat di VPC, zona ini secara otomatis bersifat pribadi dan Anda tidak boleh mengatur parameter - HostedZoneConfig _PrivateZone .

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- Untuk detail API, lihat [CreateHostedZone](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **DeleteHostedZone** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan `DeleteHostedZone`.

CLI

AWS CLI

Untuk menghapus zona yang dihosting

`delete-hosted-zone` Perintah berikut menghapus zona yang dihosting dengan id dari `Z36KTIQEXAMPLE`:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Untuk detail API, lihat [DeleteHostedZone](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Menghapus zona yang dihosting dengan ID yang ditentukan. Anda akan diminta konfirmasi sebelum perintah dilanjutkan kecuali Anda menambahkan parameter sakelar - Force.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Untuk detail API, lihat [DeleteHostedZone](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Menghapus zona yang dihosting dengan ID yang ditentukan. Anda akan diminta konfirmasi sebelum perintah dilanjutkan kecuali Anda menambahkan parameter sakelar - Force.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Untuk detail API, lihat [DeleteHostedZone](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **GetHostedZone** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan `GetHostedZone`.

CLI

AWS CLI

Untuk mendapatkan informasi tentang zona yang dihosting

`get-hosted-zone` Perintah berikut mendapatkan informasi tentang zona yang dihosting dengan id dari `Z1R8UBAEXAMPLE`:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Untuk detail API, lihat [GetHostedZone](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Mengembalikan rincian zona yang dihosting dengan ID `PJN98 FT9 Z1D633`.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Untuk detail API, lihat [GetHostedZone](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Mengembalikan rincian zona yang dihosting dengan ID `PJN98 FT9 Z1D633`.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Untuk detail API, lihat [GetHostedZone](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ListHostedZones** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListHostedZones`.

CLI

AWS CLI

Untuk membuat daftar zona yang dihosting yang terkait dengan AWS akun saat ini

`list-hosted-zones` Perintah berikut mencantumkan informasi ringkasan tentang 100 zona host pertama yang terkait dengan AWS akun saat ini. :

```
aws route53 list-hosted-zones
```

Jika Anda memiliki lebih dari 100 zona yang dihosting, atau jika Anda ingin mencantumkannya dalam grup yang lebih kecil dari 100, sertakan `--max-items` parameternya. Misalnya, untuk membuat daftar zona yang dihosting satu per satu, gunakan perintah berikut:

```
aws route53 list-hosted-zones --max-items 1
```

Untuk melihat informasi tentang zona host berikutnya, ambil nilai `NextToken` dari respon ke perintah sebelumnya, dan sertakan dalam `--starting-token` parameter, misalnya:

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Untuk detail API, lihat [ListHostedZones](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Mengeluarkan semua zona host publik dan pribadi Anda.

```
Get-R53HostedZoneList
```

Contoh 2: Mengeluarkan semua zona yang dihosting yang terkait dengan kumpulan delegasi yang dapat digunakan kembali yang memiliki ID X2CISAMPLE NZ8

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Untuk detail API, lihat [ListHostedZones](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Mengeluarkan semua zona host publik dan pribadi Anda.

```
Get-R53HostedZoneList
```

Contoh 2: Mengeluarkan semua zona yang dihosting yang terkait dengan kumpulan delegasi yang dapat digunakan kembali yang memiliki ID X2CISAMPLE NZ8

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Untuk detail API, lihat [ListHostedZones](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Rust

SDK for Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;
```

```
println!("Zones:");

for hz in hosted_zones.hosted_zones() {
    let zone_name = hz.name();
    let zone_id = hz.id();

    println!(" ID : {}", zone_id);
    println!(" Name : {}", zone_name);
    println!();
}

Ok(())
}
```

- Untuk detail API, lihat [ListHostedZones](#) referensi AWS SDK for Rust API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ListHostedZonesByName** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan `ListHostedZonesByName`.

CLI

AWS CLI

Perintah berikut mencantumkan hingga 100 zona yang dihosting yang diurutkan berdasarkan nama domain:

```
aws route53 list-hosted-zones-by-name
```

Output:

```
{
  "HostedZones": [
    {
      "ResourceRecordSetCount": 2,
      "CallerReference": "test20150527-2",
      "Config": {
```



```

        "Comment": "test2",
        "PrivateZone": false
    },
    "Id": "/hostedzone/Z119WBBTVP5WFX",
    "Name": "2.example.com."
},
{
    "ResourceRecordSetCount": 2,
    "CallerReference": "test20150527-1",
    "Config": {
        "Comment": "test",
        "PrivateZone": false
    },
    "Id": "/hostedzone/Z3P5QSUBK4P0TI",
    "Name": "www.example.com."
}
],
"IsTruncated": false,
"MaxItems": "100"
}

```

Perintah berikut mencantumkan zona yang dihosting yang diurutkan berdasarkan nama, dimulai dengan `www.example.com`:

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Output:

```

{
  "HostedZones": [
    {
      "ResourceRecordSetCount": 2,
      "CallerReference": "mwunderl20150527-1",
      "Config": {
        "Comment": "test",
        "PrivateZone": false
      },
      "Id": "/hostedzone/Z3P5QSUBK4P0TI",
      "Name": "www.example.com."
    }
  ],
  "DNSName": "www.example.com",
  "IsTruncated": false,

```

```
"MaxItems": "100"  
}
```

- Untuk detail API, lihat [ListHostedZonesByName](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Mengembalikan semua zona host publik dan pribadi Anda dalam urutan ASCII berdasarkan nama domain.

```
Get-R53HostedZonesByName
```

Contoh 2: Mengembalikan zona host publik dan pribadi Anda, dalam urutan ASCII berdasarkan nama domain, dimulai dari nama DNS yang ditentukan.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Untuk detail API, lihat [ListHostedZonesByName](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Mengembalikan semua zona host publik dan pribadi Anda dalam urutan ASCII berdasarkan nama domain.

```
Get-R53HostedZonesByName
```

Contoh 2: Mengembalikan zona host publik dan pribadi Anda, dalam urutan ASCII berdasarkan nama domain, dimulai dari nama DNS yang ditentukan.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Untuk detail API, lihat [ListHostedZonesByName](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ListQueryLoggingConfigs** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan `ListQueryLoggingConfigs`.

CLI

AWS CLI

Untuk membuat daftar konfigurasi pencatatan kueri

`list-query-logging-configs` Contoh berikut mencantumkan informasi tentang 100 konfigurasi pencatatan kueri pertama di AWS akun Anda, untuk zona `Z10X3WQEXAMPLE` yang dihosting.

```
aws route53 list-query-logging-configs \
  --hosted-zone-id Z10X3WQEXAMPLE
```

Output:

```
{
  "QueryLoggingConfigs": [
    {
      "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
      "HostedZoneId": "Z10X3WQEXAMPLE",
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/route53/example.com:*"
    }
  ]
}
```

Untuk informasi selengkapnya, lihat [Mencatat kueri DNS di Panduan](#) Pengembang Amazon Route 53.

- Untuk detail API, lihat [ListQueryLoggingConfigs](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengembalikan semua konfigurasi untuk pencatatan kueri DNS yang terkait dengan arus. Akun AWS

```
Get-R53QueryLoggingConfigList
```

Output:

Id	HostedZoneId	CloudWatchLogsLogGroupArn
--	-----	-----
59b0fa33-4fea-4471-a88c-926476aaa40d	Z385PDS6EAAAZR	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063	Z94SJHBV1AAAAZ	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b	Z3MEQ8T7AAA1BF	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example3.com:*

- Untuk detail API, lihat [ListQueryLoggingConfigs](#) di Referensi AWS Tools for PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengembalikan semua konfigurasi untuk pencatatan kueri DNS yang terkait dengan arus. Akun AWS

```
Get-R53QueryLoggingConfigList
```

Output:

Id	HostedZoneId	CloudWatchLogsLogGroupArn
--	-----	-----
59b0fa33-4fea-4471-a88c-926476aaa40d	Z385PDS6EAAAZR	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063	Z94SJHBV1AAAAZ	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b	Z3MEQ8T7AAA1BF	arn:aws:logs:us-east-1:111111111112:log-group:/aws/route53/example3.com:*

- Untuk detail API, lihat [ListQueryLoggingConfigs](#) di Referensi AWS Tools for PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh kode untuk pendaftaran domain Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan pendaftaran domain Route 53 dengan kit pengembangan AWS perangkat lunak (SDK).

Dasar-dasar adalah contoh kode yang menunjukkan kepada Anda bagaimana melakukan operasi penting dalam suatu layanan.

Tindakan merupakan kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Sementara tindakan menunjukkan cara memanggil fungsi layanan individual, Anda dapat melihat tindakan dalam konteks dalam skenario terkait.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh kode

- [Contoh dasar untuk pendaftaran domain Route 53 menggunakan AWS SDKs](#)
 - [Hello Route 53 pendaftaran domain](#)
 - [Pelajari dasar-dasar pendaftaran domain Route 53 dengan AWS SDK](#)
 - [Tindakan untuk pendaftaran domain Route 53 menggunakan AWS SDKs](#)
 - [Gunakan CheckDomainAvailability dengan AWS SDK atau CLI](#)
 - [Gunakan CheckDomainTransferability dengan AWS SDK atau CLI](#)
 - [Gunakan GetDomainDetail dengan AWS SDK atau CLI](#)
 - [Gunakan GetDomainSuggestions dengan AWS SDK atau CLI](#)
 - [Gunakan GetOperationDetail dengan AWS SDK atau CLI](#)
 - [Gunakan ListDomains dengan AWS SDK atau CLI](#)
 - [Gunakan ListOperations dengan AWS SDK atau CLI](#)
 - [Gunakan ListPrices dengan AWS SDK](#)
 - [Gunakan RegisterDomain dengan AWS SDK atau CLI](#)
 - [Gunakan ViewBilling dengan AWS SDK atau CLI](#)

Contoh dasar untuk pendaftaran domain Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan dasar-dasar Amazon Route 53 domain registration dengan AWS SDKs.

Contoh

- [Hello Route 53 pendaftaran domain](#)
- [Pelajari dasar-dasar pendaftaran domain Route 53 dengan AWS SDK](#)
- [Tindakan untuk pendaftaran domain Route 53 menggunakan AWS SDKs](#)
 - [Gunakan CheckDomainAvailability dengan AWS SDK atau CLI](#)
 - [Gunakan CheckDomainTransferability dengan AWS SDK atau CLI](#)
 - [Gunakan GetDomainDetail dengan AWS SDK atau CLI](#)
 - [Gunakan GetDomainSuggestions dengan AWS SDK atau CLI](#)
 - [Gunakan GetOperationDetail dengan AWS SDK atau CLI](#)
 - [Gunakan ListDomains dengan AWS SDK atau CLI](#)
 - [Gunakan ListOperations dengan AWS SDK atau CLI](#)
 - [Gunakan ListPrices dengan AWS SDK](#)
 - [Gunakan RegisterDomain dengan AWS SDK atau CLI](#)
 - [Gunakan ViewBilling dengan AWS SDK atau CLI](#)

Hello Route 53 pendaftaran domain

Contoh kode berikut menunjukkan cara memulai menggunakan pendaftaran domain Route 53.

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
        the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
        profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
            host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
        { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
        for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"Registration:
            {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"Renewal: {comPrices.RenewalPrice?.Price}
            {comPrices.RenewalPrice?.Currency}");
        }
    }
}

```

- Untuk detail API, lihat [ListPrices](#) di Referensi AWS SDK for .NET API.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the "com" type
 * and displays the prices for Registration and Renewal.
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
    "-");

    public static void main(String[] args) {
        final String usage = "\n" +
            "Usage:\n" +
            "    <hostedZoneId> \n\n" +
            "Where:\n" +
```



```

        "    hostedZoneId - The id value of an existing hosted zone. \n";

    if (args.length != 1) {
        System.out.println(usage);
        System.exit(1);
    }

    String domainType = args[0];
    Region region = Region.US_EAST_1;
    Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
        .region(region)
        .build();

    System.out.println(DASHES);
    System.out.println("Invokes ListPrices for at least one domain type.");
    listPrices(route53DomainsClient, domainType);
    System.out.println(DASHES);
}

public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
    try {
        ListPricesRequest pricesRequest = ListPricesRequest.builder()
            .maxItems(10)
            .tld(domainType)
            .build();

        ListPricesResponse response =
route53DomainsClient.listPrices(pricesRequest);
        List<DomainPrice> prices = response.prices();
        for (DomainPrice pr : prices) {
            System.out.println("Name: " + pr.name());
            System.out.println(
                "Registration: " + pr.registrationPrice().price() + " " +
pr.registrationPrice().currency());
            System.out.println("Renewal: " + pr.renewalPrice().price() + " "
+ pr.renewalPrice().currency());
            System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
            System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
            System.out.println("Change Ownership: " +
pr.changeOwnershipPrice().price() + " "

```

```

        + pr.changeOwnershipPrice().currency());
        System.out.println(
            "Restoration: " + pr.restorationPrice().price() + " " +
pr.restorationPrice().currency());
        System.out.println(" ");
    }

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}

```

- Untuk detail API, lihat [ListPrices](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
*/
suspend fun main(args: Array<String>) {
    val usage = ""
    Usage:
        <domainType>

    Where:
        domainType - The domain type (for example, com).

```

```

    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
                ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
                ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
                ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
                ${pr.restorationPrice?.currency}")
            }
        }
    }
}

```

- Untuk detail API, lihat [ListPrices](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Pelajari dasar-dasar pendaftaran domain Route 53 dengan AWS SDK

Contoh-contoh kode berikut menunjukkan cara:

- Buat daftar domain saat ini, dan daftar operasi dalam satu tahun terakhir.
- Lihat tagihan selama setahun terakhir, dan lihat harga untuk jenis domain.
- Dapatkan saran domain.
- Periksa ketersediaan domain dan transferabilitas.
- Secara opsional, minta pendaftaran domain.
- Dapatkan detail operasi.
- Secara opsional, dapatkan detail domain.

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkap dan pelajari cara menyiapkan dan menjalankan di [Repositori Contoh Kode AWS](#).

Jalankan skenario interaktif di penggugah/prompt perintah.

```
public static class Route53DomainScenario
{
    /*
        Before running this .NET code example, set up your development environment,
        including your credentials.

        This .NET example performs the following tasks:
        1. List current domains.
        2. List operations in the past year.
        3. View billing for the account in the past year.
```

```

    4. View prices for domain types.
    5. Get domain suggestions.
    6. Check domain availability.
    7. Check domain transferability.
    8. Optionally, request a domain registration.
    9. Get an operation detail.
    10. Optionally, get a domain detail.
*/

private static Route53Wrapper _route53Wrapper = null!;
private static IConfiguration _configuration = null!;

static async Task Main(string[] args)
{
    // Set up dependency injection for the Amazon service.
    using var host = Host.CreateDefaultBuilder(args)
        .ConfigureLogging(logging =>
            logging.AddFilter("System", LogLevel.Debug)
                .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
        .ConfigureServices((_, services) =>
            services.AddAWSService<IAmazonRoute53Domains>()
                .AddTransient<Route53Wrapper>()
            )
        .Build();

    _configuration = new ConfigurationBuilder()
        .SetBasePath(Directory.GetCurrentDirectory())
        .AddJsonFile("settings.json") // Load settings from .json file.
        .AddJsonFile("settings.local.json",
            true) // Optionally, load local settings.
        .Build();

    var logger = LoggerFactory.Create(builder =>
    {
        builder.AddConsole();
    }).CreateLogger(typeof(Route53DomainScenario));

    _route53Wrapper = host.Services.GetRequiredService<Route53Wrapper>();

    Console.WriteLine(new string('-', 80));

```

```

        Console.WriteLine("Welcome to the Amazon Route 53 domains example
scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            await ListDomains();
            await ListOperations();
            await ListBillingRecords();
            await ListPrices();
            await ListDomainSuggestions();
            await CheckDomainAvailability();
            await CheckDomainTransferability();
            var operationId = await RequestDomainRegistration();
            await GetOperationalDetail(operationId);
            await GetDomainDetails();
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("The Amazon Route 53 domains example scenario is
complete.");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List account registered domains.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomains()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"1. List account domains.");
        var domains = await _route53Wrapper.ListDomains();
        for (int i = 0; i < domains.Count; i++)
        {
            Console.WriteLine($"  {i + 1}. {domains[i].DomainName}");
        }

        if (!domains.Any())
        {

```

```
        Console.WriteLine("\tNo domains found in this account.");
    }

    Console.WriteLine(new string('-', 80));
}

/// <summary>
/// List domain operations in the past year.
/// </summary>
/// <returns>Async task.</returns>
private static async Task ListOperations()
{
    Console.WriteLine(new string('-', 80));
    Console.WriteLine($"2. List account domain operations in the past
year.");
    var operations = await _route53Wrapper.ListOperations(
        DateTime.Today.AddYears(-1));
    for (int i = 0; i < operations.Count; i++)
    {
        Console.WriteLine($"    \tOperation Id: {operations[i].OperationId}");
        Console.WriteLine($"    \tStatus: {operations[i].Status}");
        Console.WriteLine($"    \tDate: {operations[i].SubmittedDate}");
    }
    Console.WriteLine(new string('-', 80));
}

/// <summary>
/// List billing in the past year.
/// </summary>
/// <returns>Async task.</returns>
private static async Task ListBillingRecords()
{
    Console.WriteLine(new string('-', 80));
    Console.WriteLine($"3. View billing for the account in the past year.");
    var billingRecords = await _route53Wrapper.ViewBilling(
        DateTime.Today.AddYears(-1),
        DateTime.Today);
    for (int i = 0; i < billingRecords.Count; i++)
    {
        Console.WriteLine($"    \tBill Date:
{billingRecords[i].BillDate.ToShortDateString()}");
        Console.WriteLine($"    \tOperation: {billingRecords[i].Operation}");
        Console.WriteLine($"    \tPrice: {billingRecords[i].Price}");
    }
}
```

```
        if (!billingRecords.Any())
        {
            Console.WriteLine("\tNo billing records found in this account for the
past year.");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List prices for a few domain types.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListPrices()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. View prices for domain types.");
        var domainTypes = new List<string> { "net", "com", "org", "co" };

        var prices = await _route53Wrapper.ListPrices(domainTypes);
        foreach (var pr in prices)
        {
            Console.WriteLine($"    \tName: {pr.Name}");
            Console.WriteLine($"    \tRegistration: {pr.RegistrationPrice?.Price}
{pr.RegistrationPrice?.Currency}");
            Console.WriteLine($"    \tRenewal: {pr.RenewalPrice?.Price}
{pr.RenewalPrice?.Currency}");
            Console.WriteLine($"    \tTransfer: {pr.TransferPrice?.Price}
{pr.TransferPrice?.Currency}");
            Console.WriteLine($"    \tChange Ownership:
{pr.ChangeOwnershipPrice?.Price} {pr.ChangeOwnershipPrice?.Currency}");
            Console.WriteLine($"    \tRestoration: {pr.RestorationPrice?.Price}
{pr.RestorationPrice?.Currency}");
            Console.WriteLine();
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain suggestions for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomainSuggestions()
    {
        Console.WriteLine(new string('-', 80));
```



```
        Console.WriteLine($"5. Get domain suggestions.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrEmpty(domainName))
        {
            Console.WriteLine($"Enter a domain name to get available domain suggestions.");
            domainName = Console.ReadLine();
        }

        var suggestions = await _route53Wrapper.GetDomainSuggestions(domainName, true, 5);
        foreach (var suggestion in suggestions)
        {
            Console.WriteLine($"\\tSuggestion Name: {suggestion.DomainName}");
            Console.WriteLine($"\\tAvailability: {suggestion.Availability}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check availability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainAvailability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Check domain availability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrEmpty(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain availability.");
            domainName = Console.ReadLine();
        }

        var availability = await
        _route53Wrapper.CheckDomainAvailability(domainName);
        Console.WriteLine($"\\tAvailability: {availability}");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
```

```

    /// <returns>Async task.</returns>
    private static async Task CheckDomainTransferability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Check domain transferability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrEmpty(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
transferability.");
            domainName = Console.ReadLine();
        }

        var transferability = await
_route53Wrapper.CheckDomainTransferability(domainName);
        Console.WriteLine($"\\tTransferability: {transferability}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> RequestDomainRegistration()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. Optionally, request a domain registration.");

        Console.WriteLine($"\\tNote: This example uses domain request settings in
settings.json.");
        Console.WriteLine($"\\tTo change the domain registration settings, set the
values in that file.");
        Console.WriteLine($"\\tRemember, registering an actual domain will incur
an account billing cost.");
        Console.WriteLine($"\\tWould you like to begin a domain registration? (y/
n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string domainName = _configuration["DomainName"];
            ContactDetail contact = new ContactDetail();

```

```

        contact.CountryCode =
CountryCode.FindValue(_configuration["Contact:CountryCode"]);
        contact.ContactType =
ContactType.FindValue(_configuration["Contact:ContactType"]);

        _configuration.GetSection("Contact").Bind(contact);

        var operationId = await _route53Wrapper.RegisterDomain(
            domainName,
            Convert.ToBoolean(_configuration["AutoRenew"]),
            Convert.ToInt32(_configuration["DurationInYears"]),
            contact);
        if (operationId != null)
        {
            Console.WriteLine(
                $"\\tRegistration requested. Operation Id: {operationId}");
        }

        return operationId;
    }

    Console.WriteLine(new string('-', 80));
    return null;
}

/// <summary>
/// Get details for an operation.
/// </summary>
/// <returns>Async task.</returns>
private static async Task GetOperationalDetail(string? operationId)
{
    Console.WriteLine(new string('-', 80));
    Console.WriteLine($"9. Get an operation detail.");

    var operationDetails =
        await _route53Wrapper.GetOperationDetail(operationId);

    Console.WriteLine(operationDetails);

    Console.WriteLine(new string('-', 80));
}

/// <summary>
/// Optionally, get details for a registered domain.

```

```

    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> GetDomainDetails()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Get details on a domain.");

        Console.WriteLine($"\\tNote: you must have a registered domain to get
details.");
        Console.WriteLine($"\\tWould you like to get domain details? (y/n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string? domainName = null;
            while (domainName == null)
            {
                Console.WriteLine($"\\tEnter a domain name to get details.");
                domainName = Console.ReadLine();
            }

            var domainDetails = await
_route53Wrapper.GetDomainDetail(domainName);
            Console.WriteLine(domainDetails);
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }
}

```

Metode pembungkus yang digunakan oleh skenario untuk tindakan pendaftaran domain Route 53.

```

public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
ILogger<Route53Wrapper> logger)
    {

```

```
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }

    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }

    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Availability.Value;
    }

    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
```

```

    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }

    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }

    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)

```

```

    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\\tOperation {operationId}:\\n" +
                $"\\tFor domain {operationDetails.DomainName} on " +
                {operationDetails.SubmittedDate.ToShortDateString()}."\\n" +
                $"\\tMessage is {operationDetails.Message}.\\n" +
                $"\\tStatus is {operationDetails.Status}.\\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }

    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
and tech contacts.
        try

```

```

    {
        var result = await _amazonRoute53Domains.RegisterDomainAsync(
            new RegisterDomainRequest()
            {
                AdminContact = contact,
                RegistrantContact = contact,
                TechContact = contact,
                DomainName = domainName,
                AutoRenew = autoRenew,
                DurationInYears = duration,
                PrivacyProtectAdminContact = false,
                PrivacyProtectRegistrantContact = false,
                PrivacyProtectTechContact = false
            }
        );
        return result.OperationId;
    }
    catch (InvalidInputException)
    {
        _logger.LogInformation($"Unable to request registration for domain
{domainName}");
        return null;
    }
}

/// <summary>
/// View billing records for the account between a start and end date.
/// </summary>
/// <param name="startDate">The start date for billing results.</param>
/// <param name="endDate">The end date for billing results.</param>
/// <returns>A collection of billing records.</returns>
public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
{
    var results = new List<BillingRecord>();
    var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
        new ViewBillingRequest()
        {
            Start = startDate,
            End = endDate
        });

    // Get the entire list using the paginator.

```



```
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }

    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
        }
        return results;
    }

    /// <summary>
    /// List operations for the account that are submitted after a specified
    date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
```

```

        {
            results.Add(operations);
        }
        return results;
    }

    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\\tDomain {domainName}:\\n" +
                $"\\tCreated on {result.CreationDate.ToShortDateString()}\\n" +
                $"\\tAdmin contact is {result.AdminContact.Email}\\n" +
                $"\\tAuto-renew is {result.AutoRenew}\\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
}

```

- Untuk detail API, lihat topik berikut di Referensi API AWS SDK for .NET .
 - [CheckDomainAvailability](#)
 - [CheckDomainTransferability](#)
 - [GetDomainDetail](#)
 - [GetDomainSuggestions](#)

- [GetOperationDetail](#)
- [ListDomains](#)
- [ListOperations](#)
- [ListPrices](#)
- [RegisterDomain](#)
- [ViewBilling](#)

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkap dan pelajari cara menyiapkan dan menjalankan di [Repositori Contoh Kode AWS](#).

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
 * pagination.html
 *
 * This Java code example performs the following operations:
 *
 * 1. List current domains.
 * 2. List operations in the past year.
 * 3. View billing for the account in the past year.
```

```

* 4. View prices for domain types.
* 5. Get domain suggestions.
* 6. Check domain availability.
* 7. Check domain transferability.
* 8. Request a domain registration.
* 9. Get operation details.
* 10. Optionally, get domain details.
*/

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
    "-");

    public static void main(String[] args) {
        final String usage = ""

            Usage:
                <domainType> <phoneNumber> <email> <domainSuggestion>
<firstName> <lastName> <city>

            Where:
                domainType - The domain type (for example, com).\s
                phoneNumber - The phone number to use (for example,
+91.9966564xxx)      email - The email address to use.      domainSuggestion -
The domain suggestion (for example, findmy.accountants).\s
                firstName - The first name to use to register a domain.\s
                lastName - The last name to use to register a domain.\s
                city - the city to use to register a domain.\s
                """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        String phoneNumber = args[1];
        String email = args[2];
        String domainSuggestion = args[3];
        String firstName = args[4];
        String lastName = args[5];
        String city = args[6];
        Region region = Region.US_EAST_1;
    }
}

```

```
Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
    .region(region)
    .build();

System.out.println(DASHES);
System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("1. List current domains.");
listDomains(route53DomainsClient);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("2. List operations in the past year.");
listOperations(route53DomainsClient);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("3. View billing for the account in the past year.");
listBillingRecords(route53DomainsClient);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("4. View prices for domain types.");
listPrices(route53DomainsClient, domainType);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("5. Get domain suggestions.");
listDomainSuggestions(route53DomainsClient, domainSuggestion);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("6. Check domain availability.");
checkDomainAvailability(route53DomainsClient, domainSuggestion);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("7. Check domain transferability.");
checkDomainTransferability(route53DomainsClient, domainSuggestion);
System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
            domainSuggestion, phoneNumber, email, firstName,
            lastName, city);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain xxxxxxxx not found in xxxxxxxx account.");
        getDomainDetails(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
    }

    public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                .domainName(domainSuggestion)
                .build();

            GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
            System.out.println("The contact first name is " +
response.registrantContact().firstName());
            System.out.println("The contact last name is " +
response.registrantContact().lastName());
            System.out.println("The contact org name is " +
response.registrantContact().organizationName());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

```
}

    public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
        try {
            GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                .operationId(operationId)
                .build();

            GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
            System.out.println("Operation detail message is " +
response.message());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
        String domainSuggestion,
        String phoneNumber,
        String email,
        String firstName,
        String lastName,
        String city) {

        try {
            ContactDetail contactDetail = ContactDetail.builder()
                .contactType(ContactType.COMPANY)
                .state("LA")
                .countryCode(CountryCode.IN)
                .email(email)
                .firstName(firstName)
                .lastName(lastName)
                .city(city)
                .phoneNumber(phoneNumber)
                .organizationName("My Org")
                .addressLine1("My Address")
                .zipCode("123 123")
                .build();
```

```
        RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
            .adminContact(contactDetail)
            .registrantContact(contactDetail)
            .techContact(contactDetail)
            .domainName(domainSuggestion)
            .autoRenew(true)
            .durationInYears(1)
            .build();

        RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
        System.out.println("Registration requested. Operation Id: " +
response.operationId());
        return response.operationId();

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}

public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
            .domainName(domainSuggestion)
            .build();

        CheckDomainTransferabilityResponse response = route53DomainsClient
            .checkDomainTransferability(transferabilityRequest);
        System.out.println("Transferability: " +
response.transferability().transferable().toString());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
```



```
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
                CheckDomainAvailabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
                response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomainSuggestions(Route53DomainsClient
        route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainSuggestionsRequest suggestionsRequest =
                GetDomainSuggestionsRequest.builder()
                    .domainName(domainSuggestion)
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();

            GetDomainSuggestionsResponse response =
                route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
                    suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

```
public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
    try {
        ListPricesRequest pricesRequest = ListPricesRequest.builder()
            .tld(domainType)
            .build();

        ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
        listRes.stream()
            .flatMap(r -> r.prices().stream())
            .forEach(content -> System.out.println(" Name: " +
content.name() +
                " Registration: " +
content.registrationPrice().price() + " "
                + content.registrationPrice().currency() +
                " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        LocalDateTime localDateTime2 = localDateTime.minusYears(1);
        Instant myStartTime = localDateTime2.toInstant(zoneOffset);
        Instant myEndTime = localDateTime.toInstant(zoneOffset);

        ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
            .start(myStartTime)
            .end(myEndTime)
            .build();

        ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
        listRes.stream()
```

```

        .flatMap(r -> r.billingRecords().stream())
        .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
            " Operation: " + content.operationAsString() +
            " Price: " + content.price()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listOperations(Route53DomainsClient route53DomainsClient)
{
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        localDateTime = localDateTime.minusYears(1);
        Instant myTime = localDateTime.toInstant(zoneOffset);

        ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
            .submittedSince(myTime)
            .build();

        ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
        listRes.stream()
            .flatMap(r -> r.operations().stream())
            .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                " Status: " + content.statusAsString() +
                " Date: " + content.submittedDate()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listDomains(Route53DomainsClient route53DomainsClient) {
    try {

```

```
        ListDomainsIterable listRes =
route53DomainsClient.listDomainsPaginator();
        listRes.stream()
            .flatMap(r -> r.domains().stream())
            .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
```

- Untuk detail API, lihat topik berikut di Referensi API AWS SDK for Java 2.x .
 - [CheckDomainAvailability](#)
 - [CheckDomainTransferability](#)
 - [GetDomainDetail](#)
 - [GetDomainSuggestions](#)
 - [GetOperationDetail](#)
 - [ListDomains](#)
 - [ListOperations](#)
 - [ListPrices](#)
 - [RegisterDomain](#)
 - [ViewBilling](#)

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkap dan pelajari cara menyiapkan dan menjalankan di [Repositori Contoh Kode AWS](#).

```
/**
```

Before running this Kotlin code example, set up your development environment, including your credentials.

For more information, see the following documentation topic:

<https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html>

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.

```
*/
```

```
val DASHES: String = String(CharArray(80)).replace("\u0000", "-")
```

```
suspend fun main(args: Array<String>) {
```

```
    val usage = ""
```

```
        Usage:
```

```
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
```

```
<lastName> <city>
```

```
        Where:
```

```
            domainType - The domain type (for example, com).
```

```
            phoneNumber - The phone number to use (for example, +1.2065550100)
```

```
            email - The email address to use.
```

```
            domainSuggestion - The domain suggestion (for example, findmy.example).
```

```
            firstName - The first name to use to register a domain.
```

```
            lastName - The last name to use to register a domain.
```

```
            city - The city to use to register a domain.
```

```
    ""
```

```
    if (args.size != 7) {
```

```
        println(usage)
```

```
        exitProcess(1)
    }

    val domainType = args[0]
    val phoneNumber = args[1]
    val email = args[2]
    val domainSuggestion = args[3]
    val firstName = args[4]
    val lastName = args[5]
    val city = args[6]

    println(DASHES)
    println("Welcome to the Amazon Route 53 domains example scenario.")
    println(DASHES)

    println(DASHES)
    println("1. List current domains.")
    listDomains()
    println(DASHES)

    println(DASHES)
    println("2. List operations in the past year.")
    listOperations()
    println(DASHES)

    println(DASHES)
    println("3. View billing for the account in the past year.")
    listBillingRecords()
    println(DASHES)

    println(DASHES)
    println("4. View prices for domain types.")
    listAllPrices(domainType)
    println(DASHES)

    println(DASHES)
    println("5. Get domain suggestions.")
    listDomainSuggestions(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("6. Check domain availability.")
    checkDomainAvailability(domainSuggestion)
    println(DASHES)
```

```

println(DASHES)
println("7. Check domain transferability.")
checkDomainTransferability(domainSuggestion)
println(DASHES)

println(DASHES)
println("8. Request a domain registration.")
val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
firstName, lastName, city)
println(DASHES)

println(DASHES)
println("9. Get operation details.")
getOperationalDetail(opId)
println(DASHES)

println(DASHES)
println("10. Get domain details.")
println("Note: You must have a registered domain to get details.")
println("Otherwise an exception is thrown that states ")
println("Domain xxxxxxxx not found in xxxxxxxx account.")
getDomainDetails(domainSuggestion)
println(DASHES)
}

suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
${response.registrantContact?.firstName}")
        println("The contact last name is
${response.registrantContact?.lastName}")
        println("The contact org name is
${response.registrantContact?.organizationName}")
    }
}

suspend fun getOperationalDetail(opId: String?) {

```

```
val detailRequest =
    GetOperationDetailRequest {
        operationId = opId
    }
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response = route53DomainsClient.getOperationDetail(detailRequest)
    println("Operation detail message is ${response.message}")
}

suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }
}
```



```
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response = route53DomainsClient.registerDomain(domainRequest)
    println("Registration requested. Operation Id: ${response.operationId}")
    return response.operationId
}

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response =
            route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}

suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response =
            route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
}

suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
```

```

        val response =
            route53DomainsClient.getDomainSuggestions(suggestionsRequest)
            response.suggestionsList?.forEach { suggestion ->
                println("Suggestion Name: ${suggestion.domainName}")
                println("Availability: ${suggestion.availability}")
                println(" ")
            }
        }
    }

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
${pr.restorationPrice?.currency}")
            }
        }
    }

suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
        currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }
}

```

```

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    route53DomainsClient
        .viewBillingPaginated(viewBillingRequest)
        .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
        .collect { billing ->
            println("Bill Date: ${billing.billDate}")
            println("Operation: ${billing.operation}")
            println("Price: ${billing.price}")
        }
    }
}

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    route53DomainsClient
        .listOperationsPaginated(operationsRequest)
        .transform { it.operations?.forEach { obj -> emit(obj) } }
        .collect { content ->
            println("Operation Id: ${content.operationId}")
            println("Status: ${content.status}")
            println("Date: ${content.submittedDate}")
        }
    }
}

```

```
}

suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- Lihat detail API di topik-topik berikut dalam Referensi API AWS SDK For Kotlin.
 - [CheckDomainAvailability](#)
 - [CheckDomainTransferability](#)
 - [GetDomainDetail](#)
 - [GetDomainSuggestions](#)
 - [GetOperationDetail](#)
 - [ListDomains](#)
 - [ListOperations](#)
 - [ListPrices](#)
 - [RegisterDomain](#)
 - [ViewBilling](#)

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Tindakan untuk pendaftaran domain Route 53 menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara melakukan tindakan pendaftaran domain Route 53 individual dengan AWS SDKs. Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan instruksi untuk mengatur dan menjalankan kode.

Contoh berikut hanya mencakup tindakan yang paling umum digunakan. Untuk daftar lengkapnya, lihat [Referensi Amazon Route 53 domain registration API](#).

Contoh

- [Gunakan CheckDomainAvailability dengan AWS SDK atau CLI](#)
- [Gunakan CheckDomainTransferability dengan AWS SDK atau CLI](#)
- [Gunakan GetDomainDetail dengan AWS SDK atau CLI](#)
- [Gunakan GetDomainSuggestions dengan AWS SDK atau CLI](#)
- [Gunakan GetOperationDetail dengan AWS SDK atau CLI](#)
- [Gunakan ListDomains dengan AWS SDK atau CLI](#)
- [Gunakan ListOperations dengan AWS SDK atau CLI](#)
- [Gunakan ListPrices dengan AWS SDK](#)
- [Gunakan RegisterDomain dengan AWS SDK atau CLI](#)
- [Gunakan ViewBilling dengan AWS SDK atau CLI](#)

Gunakan **CheckDomainAvailability** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `CheckDomainAvailability`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
```

```
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- Untuk detail API, lihat [CheckDomainAvailability](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menentukan apakah Anda dapat mendaftarkan nama domain dengan Route 53

`check-domain-availability` Perintah berikut mengembalikan informasi tentang apakah nama `example.com` domain tersedia untuk didaftarkan menggunakan Route 53.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```
aws route53domains check-domain-availability \
  --region us-east-1 \
  --domain-name example.com
```

Output:

```
{
  "Availability": "UNAVAILABLE"
}
```

Route 53 mendukung sejumlah besar domain tingkat atas (TLDs), seperti `.com` dan `.jp`, tetapi kami tidak mendukung semua yang tersedia. TLDs Jika Anda memeriksa ketersediaan domain

dan Route 53 tidak mendukung TLD, akan `check-domain-availability` menampilkan pesan berikut.

An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability operation: <top-level domain> tld is not supported.

Untuk daftar yang dapat Anda gunakan saat mendaftarkan domain dengan Route 53, lihat [Domain yang Dapat Anda Daftarkan dengan Amazon Route 53](#) di Panduan Pengembang Amazon Route 53. TLDs Untuk informasi selengkapnya tentang mendaftarkan domain dengan Amazon Route 53, lihat [Mendaftarkan Domain Baru](#) di Panduan Pengembang Amazon Route 53.

- Untuk detail API, lihat [CheckDomainAvailability](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        CheckDomainAvailabilityRequest availabilityRequest =
        CheckDomainAvailabilityRequest.builder()
            .domainName(domainSuggestion)
            .build();

        CheckDomainAvailabilityResponse response = route53DomainsClient
            .checkDomainAvailability(availabilityRequest);
        System.out.println(domainSuggestion + " is " +
        response.availability().toString());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

```
}  
}
```

- Untuk detail API, lihat [CheckDomainAvailability](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun checkDomainAvailability(domainSuggestion: String) {  
    val availabilityRequest =  
        CheckDomainAvailabilityRequest {  
            domainName = domainSuggestion  
        }  
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use  
{ route53DomainsClient ->  
    val response =  
        route53DomainsClient.checkDomainAvailability(availabilityRequest)  
    println("$domainSuggestion is ${response.availability}")  
}  
}
```

- Untuk detail API, lihat [CheckDomainAvailability](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **CheckDomainTransferability** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `CheckDomainTransferability`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Check the transferability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for transferability.</param>
/// <returns>A transferability result string.</returns>
public async Task<string> CheckDomainTransferability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Transferability.Transferable.Value;
}
```

- Untuk detail API, lihat [CheckDomainTransferability](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menentukan apakah domain dapat ditransfer ke Route 53

`check-domain-transferability` Perintah berikut mengembalikan informasi tentang apakah Anda dapat mentransfer nama domain `example.com` ke Route 53.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```
aws route53domains check-domain-transferability \
  --region us-east-1 \
  --domain-name example.com
```

Output:

```
{
  "Transferability": {
    "Transferable": "UNTRANSFERABLE"
  }
}
```

Untuk informasi selengkapnya, lihat [Mentransfer Pendaftaran Domain ke Amazon Route 53](#) di Panduan Pengembang Amazon Route 53.

- Untuk detail API, lihat [CheckDomainTransferability](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        CheckDomainTransferabilityRequest transferabilityRequest =
        CheckDomainTransferabilityRequest.builder()
            .domainName(domainSuggestion)
```

```

        .build();

        CheckDomainTransferabilityResponse response = route53DomainsClient
            .checkDomainTransferability(transferabilityRequest);
        System.out.println("Transferability: " +
            response.transferability().transferable().toString());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- Untuk detail API, lihat [CheckDomainTransferability](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response =
            route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}

```

- Untuk detail API, lihat [CheckDomainTransferability](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **GetDomainDetail** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetDomainDetail`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Get details for a domain.
/// </summary>
/// <returns>A string with detail information about the domain.</returns>
public async Task<string> GetDomainDetail(string domainName)
{
    try
    {
        var result = await _amazonRoute53Domains.GetDomainDetailAsync(
            new GetDomainDetailRequest()
            {
                DomainName = domainName
            });
        var details = $"\\tDomain {domainName}:\\n" +
            $"\\tCreated on
{result.CreationDate.ToShortDateString()}\\n" +
            $"\\tAdmin contact is {result.AdminContact.Email}\\n" +
```

```

        $"\\tAuto-renew is {result.AutoRenew}\\.\\n";

        return details;
    }
    catch (InvalidInputException)
    {
        return $"Domain {domainName} was not found in your account.";
    }
}

```

- Untuk detail API, lihat [GetDomainDetail](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk mendapatkan informasi rinci tentang domain tertentu

`get-domain-detail` Perintah berikut menampilkan informasi rinci tentang domain yang ditentukan.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```

aws route53domains get-domain-detail \
  --region us-east-1 \
  --domain-name example.com

```

Output:

```

{
  "DomainName": "example.com",
  "Nameservers": [
    {
      "Name": "ns-2048.awsdns-64.com",
      "GlueIps": []
    },
    {
      "Name": "ns-2049.awsdns-65.net",
      "GlueIps": []
    }
  ],
}

```

```
{
  "Name": "ns-2050.awsdns-66.org",
  "GlueIps": []
},
{
  "Name": "ns-2051.awsdns-67.co.uk",
  "GlueIps": []
}
],
"AutoRenew": true,
"AdminContact": {
  "FirstName": "Saanvi",
  "LastName": "Sarkar",
  "ContactType": "COMPANY",
  "OrganizationName": "Example",
  "AddressLine1": "123 Main Street",
  "City": "Anytown",
  "State": "WA",
  "CountryCode": "US",
  "ZipCode": "98101",
  "PhoneNumber": "+1.8005551212",
  "Email": "ssarkar@example.com",
  "ExtraParams": []
},
"RegistrantContact": {
  "FirstName": "Alejandro",
  "LastName": "Rosalez",
  "ContactType": "COMPANY",
  "OrganizationName": "Example",
  "AddressLine1": "123 Main Street",
  "City": "Anytown",
  "State": "WA",
  "CountryCode": "US",
  "ZipCode": "98101",
  "PhoneNumber": "+1.8005551212",
  "Email": "arosalez@example.com",
  "ExtraParams": []
},
"TechContact": {
  "FirstName": "Wang",
  "LastName": "Xiulan",
  "ContactType": "COMPANY",
  "OrganizationName": "Example",
  "AddressLine1": "123 Main Street",
```

```

        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon",
    "RegistrarUrl": "http://registrar.amazon.com",
    "AbuseContactEmail": "abuse@registrar.amazon.com",
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}

```

- Untuk detail API, lihat [GetDomainDetail](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        GetDomainDetailRequest detailRequest =
        GetDomainDetailRequest.builder()
            .domainName(domainSuggestion)
            .build();
    }
}

```

```
        GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
        System.out.println("The contact first name is " +
response.registrantContact().firstName());
        System.out.println("The contact last name is " +
response.registrantContact().lastName());
        System.out.println("The contact org name is " +
response.registrantContact().organizationName());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Untuk detail API, lihat [GetDomainDetail](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    val response = route53DomainsClient.getDomainDetail(detailRequest)
    println("The contact first name is
${response.registrantContact?.firstName}")
    println("The contact last name is
${response.registrantContact?.lastName}")
}
```



```
println("The contact org name is  
${response.registrantContact?.organizationName}")  
}  
}
```

- Untuk detail API, lihat [GetDomainDetail](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **GetDomainSuggestions** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetDomainSuggestions`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>  
/// Get a list of suggestions for a given domain.  
/// </summary>  
/// <param name="domain">The domain to check for suggestions.</param>  
/// <param name="onlyAvailable">If true, only returns available domains.</  
param>  
/// <param name="suggestionCount">The number of suggestions to return.  
Defaults to the max of 50.</param>
```

```

    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
        bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }

```

- Untuk detail API, lihat [GetDomainSuggestions](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk mendapatkan daftar nama domain yang disarankan

`get-domain-suggestions` Perintah berikut menampilkan daftar nama domain yang disarankan berdasarkan nama domain `example.com`. Responsnya hanya mencakup nama domain yang tersedia. Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```

aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available

```

Output:

```

{
  "SuggestionsList": [
    {
      "DomainName": "egzaampal.com",

```

```
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "examplelaw.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "examplehouse.net",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "homeexample.net",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "examplelist.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "examplenews.net",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "officeexample.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "exampleworld.com",
        "Availability": "AVAILABLE"
    },
    {
        "DomainName": "exampleart.com",
        "Availability": "AVAILABLE"
    }
  ]
}
```

- Untuk detail API, lihat [GetDomainSuggestions](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
    try {
        GetDomainSuggestionsRequest suggestionsRequest =
        GetDomainSuggestionsRequest.builder()
            .domainName(domainSuggestion)
            .suggestionCount(5)
            .onlyAvailable(true)
            .build();

        GetDomainSuggestionsResponse response =
        route53DomainsClient.getDomainSuggestions(suggestionsRequest);
        List<DomainSuggestion> suggestions = response.suggestionsList();
        for (DomainSuggestion suggestion : suggestions) {
            System.out.println("Suggestion Name: " +
suggestion.domainName());
            System.out.println("Availability: " + suggestion.availability());
            System.out.println(" ");
        }

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Untuk detail API, lihat [GetDomainSuggestions](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {  
    val suggestionsRequest =  
        GetDomainSuggestionsRequest {  
            domainName = domainSuggestion  
            suggestionCount = 5  
            onlyAvailable = true  
        }  
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use  
    { route53DomainsClient ->  
        val response =  
            route53DomainsClient.getDomainSuggestions(suggestionsRequest)  
        response.suggestionsList?.forEach { suggestion ->  
            println("Suggestion Name: ${suggestion.domainName}")  
            println("Availability: ${suggestion.availability}")  
            println(" ")  
        }  
    }  
}
```

- Untuk detail API, lihat [GetDomainSuggestions](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **GetOperationDetail** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetOperationDetail`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Get details for a domain action operation.
/// </summary>
/// <param name="operationId">The operational Id.</param>
/// <returns>A string describing the operational details.</returns>
public async Task<string> GetOperationDetail(string? operationId)
{
    if (operationId == null)
        return "Unable to get operational details because ID is null.";
    try
    {
        var operationDetails =
            await _amazonRoute53Domains.GetOperationDetailAsync(
                new GetOperationDetailRequest
                {
                    OperationId = operationId
                }
            );

        var details = $"\\tOperation {operationId}:\\n" +
            $"\\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}\\n" +
            $"\\tMessage is {operationDetails.Message}\\n" +
            $"\\tStatus is {operationDetails.Status}\\n";
    }
}
```

```
        return details;
    }
    catch (AmazonRoute53DomainsException ex)
    {
        return $"Unable to get operation details. Here's why: {ex.Message}.";
    }
}
```

- Untuk detail API, lihat [GetOperationDetail](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk mendapatkan status operasi saat ini

Beberapa operasi pendaftaran domain beroperasi secara asinkron dan mengembalikan respons sebelum selesai. Operasi ini mengembalikan ID operasi yang dapat Anda gunakan untuk mendapatkan status saat ini. `get-operation-detail` Perintah berikut mengembalikan status operasi yang ditentukan.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```
aws route53domains get-operation-detail \
  --region us-east-1 \
  --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Output:

```
{
  "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
  "Status": "SUCCESSFUL",
  "DomainName": "example.com",
  "Type": "DOMAIN_LOCK",
  "SubmittedDate": 1573749367.864
}
```

- Untuk detail API, lihat [GetOperationDetail](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
    try {
        GetOperationDetailRequest detailRequest =
        GetOperationDetailRequest.builder()
            .operationId(operationId)
            .build();

        GetOperationDetailResponse response =
        route53DomainsClient.getOperationDetail(detailRequest);
        System.out.println("Operation detail message is " +
        response.message());

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Untuk detail API, lihat [GetOperationDetail](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).


```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}
```

- Untuk detail API, lihat [GetOperationDetail](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ListDomains** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListDomains`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/// <summary>
/// List the domains for the account.
/// </summary>
/// <returns>A collection of domain summary records.</returns>
public async Task<List<DomainSummary>> ListDomains()
{
    var results = new List<DomainSummary>();
    var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
        new ListDomainsRequest());

    // Get the entire list using the paginator.
    await foreach (var domain in paginateDomains.Domains)
    {
        results.Add(domain);
    }
    return results;
}

```

- Untuk detail API, lihat [ListDomains](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk membuat daftar domain yang terdaftar dengan akun saat ini AWS

`list-domains` Perintah berikut mencantumkan informasi ringkasan tentang domain yang terdaftar dengan AWS akun saat ini.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```

aws route53domains list-domains
  --region us-east-1

```

Output:

```

{
  "Domains": [
    {

```

```

        "DomainName": "example.com",
        "AutoRenew": true,
        "TransferLock": true,
        "Expiry": 1602712345.0
    },
    {
        "DomainName": "example.net",
        "AutoRenew": true,
        "TransferLock": true,
        "Expiry": 1602723456.0
    },
    {
        "DomainName": "example.org",
        "AutoRenew": true,
        "TransferLock": true,
        "Expiry": 1602734567.0
    }
]
}

```

- Untuk detail API, lihat [ListDomains](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

public static void listDomains(Route53DomainsClient route53DomainsClient) {
    try {
        ListDomainsIterable listRes =
            route53DomainsClient.listDomainsPaginator();
        listRes.stream()
            .flatMap(r -> r.domains().stream())
            .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));
    } catch (Route53Exception e) {

```

```
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Untuk detail API, lihat [ListDomains](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- Untuk detail API, lihat [ListDomains](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ListOperations** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListOperations`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// List operations for the account that are submitted after a specified
date.
/// </summary>
/// <returns>A collection of operation summary records.</returns>
public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
{
    var results = new List<OperationSummary>();
    var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
        new ListOperationsRequest()
        {
            SubmittedSince = submittedSince
        });

    // Get the entire list using the paginator.
    await foreach (var operations in paginateOperations.Operations)
    {
        results.Add(operations);
    }
    return results;
}
```

- Untuk detail API, lihat [ListOperations](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk mencantumkan status operasi yang mengembalikan ID operasi

Beberapa operasi pendaftaran domain berjalan secara asinkron dan mengembalikan respons sebelum selesai. Operasi ini mengembalikan ID operasi yang dapat Anda gunakan untuk mendapatkan status saat ini. `list-operations` Perintah berikut mencantumkan informasi ringkasan, termasuk status, tentang operasi registrasi domain saat ini.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```
aws route53domains list-operations
--region us-east-1
```

Output:

```
{
  "Operations": [
    {
      "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
      "Status": "SUCCESSFUL",
      "Type": "DOMAIN_LOCK",
      "SubmittedDate": 1455321739.986
    },
    {
      "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
      "Status": "SUCCESSFUL",
      "Type": "UPDATE_NAMESERVER",
      "SubmittedDate": 1468960475.109
    },
    {
      "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
      "Status": "SUCCESSFUL",
      "Type": "RENEW_DOMAIN",
      "SubmittedDate": 1473561835.943
    },
    {
      "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
      "Status": "SUCCESSFUL",
      "Type": "UPDATE_DOMAIN_CONTACT",

```

```

        "SubmittedDate": 1547501003.41
      }
    ]
  }

```

Outputnya mencakup semua operasi yang mengembalikan ID operasi dan yang telah Anda lakukan di semua domain yang pernah Anda daftarkan menggunakan AWS akun saat ini. Jika Anda hanya ingin mendapatkan operasi yang Anda kirimkan setelah tanggal yang ditentukan, Anda dapat menyertakan `submitted-since` parameter dan menentukan tanggal dalam format Unix dan Waktu Universal Terkoordinasi (UTC). Perintah berikut mendapatkan status semua operasi yang diajukan setelah pukul 12:00 UTC pada 1 Januari 2020.

```

aws route53domains list-operations \
  --submitted-since 1577836800

```

- Untuk detail API, lihat [ListOperations](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

public static void listOperations(Route53DomainsClient route53DomainsClient)
{
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        localDateTime = localDateTime.minusYears(1);
        Instant myTime = localDateTime.toInstant(zoneOffset);

        ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
            .submittedSince(myTime)

```

```

        .build();

        ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
        listRes.stream()
            .flatMap(r -> r.operations().stream())
            .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                " Status: " + content.statusAsString() +
                " Date: " + content.submittedDate()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- Untuk detail API, lihat [ListOperations](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }
}

```



```
Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    route53DomainsClient
        .listOperationsPaginated(operationsRequest)
        .transform { it.operations?.forEach { obj -> emit(obj) } }
        .collect { content ->
            println("Operation Id: ${content.operationId}")
            println("Status: ${content.status}")
            println("Date: ${content.submittedDate}")
        }
    }
}
```

- Untuk detail API, lihat [ListOperations](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ListPrices** dengan AWS SDK

Contoh kode berikut menunjukkan cara menggunakan `ListPrices`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/// <summary>
/// List prices for domain type operations.
/// </summary>
/// <param name="domainTypes">Domain types to include in the results.</param>
/// <returns>The list of domain prices.</returns>
public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
{
    var results = new List<DomainPrice>();
    var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
    // Get the entire list using the paginator.
    await foreach (var prices in paginatePrices.Prices)
    {
        results.Add(prices);
    }
    return results.Where(p => domainTypes.Contains(p.Name)).ToList();
}

```

- Untuk detail API, lihat [ListPrices](#) di Referensi AWS SDK for .NET API.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
    try {
        ListPricesRequest pricesRequest = ListPricesRequest.builder()
            .tld(domainType)
            .build();

        ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
        listRes.stream()
            .flatMap(r -> r.prices().stream())

```

```

        .forEach(content -> System.out.println(" Name: " +
content.name() +
        " Registration: " +
content.registrationPrice().price() + " "
        + content.registrationPrice().currency() +
        " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- Untuk detail API, lihat [ListPrices](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
    route53DomainsClient
        .listPricesPaginated(pricesRequest)
        .transform { it.prices?.forEach { obj -> emit(obj) } }
        .collect { pr ->
            println("Registration: ${pr.registrationPrice}
${pr.registrationPrice?.currency}")
        }
    }
}

```

```
        println("Renewal: ${pr.renewalPrice?.price}
${pr.renewalPrice?.currency}")
        println("Transfer: ${pr.transferPrice?.price}
${pr.transferPrice?.currency}")
        println("Restoration: ${pr.restorationPrice?.price}
${pr.restorationPrice?.currency}")
    }
}
}
```

- Untuk detail API, lihat [ListPrices](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **RegisterDomain** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `RegisterDomain`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Initiate a domain registration request.
/// </summary>
```

```

    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
{domainName}");
            return null;
        }
    }
}

```

- Untuk detail API, lihat [RegisterDomain](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk mendaftarkan domain

`register-domain` Perintah berikut mendaftarkan domain, mengambil semua nilai parameter dari file berformat JSON.

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```
aws route53domains register-domain \
  --region us-east-1 \
  --cli-input-json file://register-domain.json
```

Isi dari `register-domain.json`:

```
{
  "DomainName": "example.com",
  "DurationInYears": 1,
  "AutoRenew": true,
  "AdminContact": {
    "FirstName": "Martha",
    "LastName": "Rivera",
    "ContactType": "PERSON",
    "OrganizationName": "Example",
    "AddressLine1": "1 Main Street",
    "City": "Anytown",
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "mriviera@example.com"
  },
  "RegistrantContact": {
    "FirstName": "Li",
    "LastName": "Juan",
    "ContactType": "PERSON",
    "OrganizationName": "Example",
    "AddressLine1": "1 Main Street",
    "City": "Anytown",
```

```
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "ljuan@example.com"
  },
  "TechContact": {
    "FirstName": "Mateo",
    "LastName": "Jackson",
    "ContactType": "PERSON",
    "OrganizationName": "Example",
    "AddressLine1": "1 Main Street",
    "City": "Anytown",
    "State": "WA",
    "CountryCode": "US",
    "ZipCode": "98101",
    "PhoneNumber": "+1.8005551212",
    "Email": "mjackson@example.com"
  },
  "PrivacyProtectAdminContact": true,
  "PrivacyProtectRegistrantContact": true,
  "PrivacyProtectTechContact": true
}
```

Output:

```
{
  "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Untuk mengonfirmasi bahwa operasi berhasil, Anda dapat menjalankannya `get-operation-detail`. Untuk informasi selengkapnya, lihat [get-operation-detail](#).

Untuk informasi lebih lanjut, lihat [Mendaftarkan Domain Baru](#) dalam Panduan Pengembang Amazon Route 53.

Untuk informasi tentang domain tingkat atas (TLDs) mana yang memerlukan nilai `ExtraParams` dan nilai validnya, lihat [ExtraParam](#) di Referensi API Amazon Route 53.

- Untuk detail API, lihat [RegisterDomain](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
    String domainSuggestion,
    String phoneNumber,
    String email,
    String firstName,
    String lastName,
    String city) {

    try {
        ContactDetail contactDetail = ContactDetail.builder()
            .contactType(ContactType.COMPANY)
            .state("LA")
            .countryCode(CountryCode.IN)
            .email(email)
            .firstName(firstName)
            .lastName(lastName)
            .city(city)
            .phoneNumber(phoneNumber)
            .organizationName("My Org")
            .addressLine1("My Address")
            .zipCode("123 123")
            .build();

        RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
            .adminContact(contactDetail)
            .registrantContact(contactDetail)
            .techContact(contactDetail)
            .domainName(domainSuggestion)
            .autoRenew(true)
            .durationInYears(1)
            .build();
```



```

        RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
        System.out.println("Registration requested. Operation Id: " +
response.operationId());
        return response.operationId();

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}

```

- Untuk detail API, lihat [RegisterDomain](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal

```

```

        lastName = lastNameVal
        city = cityVal
        phoneNumber = phoneNumberVal
        organizationName = "My Org"
        addressLine1 = "My Address"
        zipCode = "123 123"
    }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}

```

- Untuk detail API, lihat [RegisterDomain](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **ViewBilling** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan **ViewBilling**.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Pelajari dasar-dasarnya](#)

.NET

SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// View billing records for the account between a start and end date.
/// </summary>
/// <param name="startDate">The start date for billing results.</param>
/// <param name="endDate">The end date for billing results.</param>
/// <returns>A collection of billing records.</returns>
public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
{
    var results = new List<BillingRecord>();
    var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
        new ViewBillingRequest()
        {
            Start = startDate,
            End = endDate
        });

    // Get the entire list using the paginator.
    await foreach (var billingRecords in paginateBilling.BillingRecords)
    {
        results.Add(billingRecords);
    }
    return results;
}
```

- Untuk detail API, lihat [ViewBilling](#) di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk mendapatkan informasi penagihan untuk biaya pendaftaran domain untuk akun saat ini AWS

`view-billing` Perintah berikut mengembalikan semua catatan penagihan terkait domain untuk akun saat ini untuk periode dari 1 Januari 2018 (1514764800 dalam waktu Unix) dan tengah malam pada tanggal 31 Desember 2019 (1577836800 dalam waktu Unix).

Perintah ini hanya berjalan di `us-east-1` Wilayah. Jika wilayah default Anda diatur ke `us-east-1`, Anda dapat menghilangkan `region` parameter.

```
aws route53domains view-billing \
  --region us-east-1 \
  --start-time 1514764800 \
  --end-time 1577836800
```

Output:

```
{
  "BillingRecords": [
    {
      "DomainName": "example.com",
      "Operation": "RENEW_DOMAIN",
      "InvoiceId": "149962827",
      "BillDate": 1536618063.181,
      "Price": 12.0
    },
    {
      "DomainName": "example.com",
      "Operation": "RENEW_DOMAIN",
      "InvoiceId": "290913289",
      "BillDate": 1568162630.884,
      "Price": 12.0
    }
  ]
}
```

Untuk informasi selengkapnya, lihat [ViewBilling](#) di Referensi API Amazon Route 53.

- Untuk detail API, lihat [ViewBilling](#) di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
    try {
        Date currentDate = new Date();
        LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
        ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
        LocalDateTime localDateTime2 = localDateTime.minusYears(1);
        Instant myStartTime = localDateTime2.toInstant(zoneOffset);
        Instant myEndTime = localDateTime.toInstant(zoneOffset);

        ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
            .start(myStartTime)
            .end(myEndTime)
            .build();

        ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
        listRes.stream()
            .flatMap(r -> r.billingRecords().stream())
            .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                " Operation: " + content.operationAsString() +
                " Price: " + content.price()));

    } catch (Route53Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Untuk detail API, lihat [ViewBilling](#) di Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
        currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
    { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}
```

```
}
```

- Untuk detail API, lihat [ViewBilling](#) di AWS SDK untuk referensi API Kotlin.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Menggunakan Route 53 dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Keamanan di Amazon Route 53

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Route 53, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Route 53. Topik berikut menunjukkan kepada Anda cara mengonfigurasi Route 53 untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Route 53 Anda.

Topik

- [Perlindungan data di Route 53](#)
- [Identity and access management di Amazon Route 53](#)
- [Mencatat log dan memantau di Amazon Route 53](#)
- [Validasi kepatuhan untuk Amazon Route 53](#)
- [Ketahanan di Amazon Route 53](#)
- [Keamanan Infrastruktur di Amazon Route 53](#)

Perlindungan data di Route 53

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon Route 53. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensi dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Route 53 atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Perlindungan dari catatan delegasi yang menggantung di Route 53

Dengan Route 53, pelanggan dapat membuat zona yang dihosting, seperti `example.com`, untuk meng-host catatan DNS mereka. Setiap zona yang dihosting dilengkapi dengan “set delegasi”, yang merupakan satu set dari empat server nama yang dapat digunakan pelanggan untuk mengonfigurasi catatan NS di domain induk. Catatan NS ini dapat disebut “catatan NS delegasi”, atau “catatan delegasi”.

Agar zona yang dihosting `example.com` Route 53 menjadi otoritatif, pemilik domain yang sah perlu mengonfigurasi catatan delegasi di `example.com` domain induk “.com” mereka melalui registrar domain domain. Dalam kasus di mana pelanggan kehilangan akses ke empat server nama yang dikonfigurasi dalam domain induk, misalnya karena zona host terkait dihapus, itu dapat menciptakan risiko bahwa penyerang dapat mengeksploitasi. Ini disebut sebagai risiko “catatan delegasi yang menggantung”.

Route 53 melindungi dari risiko catatan delegasi yang menggantung dalam kasus di mana zona yang dihosting dihapus. Setelah penghapusan, jika zona host baru dibuat dengan nama domain yang sama, Route 53 akan memeriksa apakah catatan delegasi yang menunjuk ke zona host yang dihapus masih ada di domain induk. Jika ya, Route 53 akan mencegah server nama yang tumpang tindih ditetapkan. Ini adalah skenario 1 dalam contoh berikut.

Namun, ada risiko catatan delegasi menggantung lainnya, yang tidak dapat dilindungi oleh Route 53, seperti yang dijelaskan dalam skenario 2 dan 3 dalam contoh berikut. Untuk melindungi diri Anda dari serangkaian risiko yang lebih luas ini, pastikan catatan NS induk cocok dengan delegasi yang ditetapkan untuk zona yang dihosting Route 53. Anda dapat menemukan kumpulan delegasi zona yang dihosting melalui konsol Route 53 atau AWS CLI. Untuk informasi selengkapnya, lihat [Mencantumkan catatan](#) atau [get-hosted-zone](#).

Selain itu, mengaktifkan penandatanganan DNSSEC untuk zona host Route 53 dapat berfungsi sebagai lapisan perlindungan lain di luar praktik terbaik yang disebutkan di atas. DNSSEC mengotentikasi bahwa jawaban DNS berasal dari sumber otoritatif, yang secara efektif melindungi terhadap risiko ini. Untuk mengetahui informasi selengkapnya, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

Contoh

Dalam contoh berikut, kami berasumsi Anda memiliki domain `example.com`, dan domain turunannya `child.example.com`. Kami akan menjelaskan bagaimana dalam berbagai skenario catatan delegasi yang menggantung dapat dibuat, bagaimana Route 53 melindungi domain Anda dari penyalahgunaan dan cara mengurangi risiko yang terkait dengan catatan delegasi yang menggantung secara efektif.

Skenario 1:

Anda membuat zona yang dihosting `child.example.com` dengan empat server nama: `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>`. `<ns4>` Anda mengatur delegasi dengan benar di zona yang dihosting `example.com`, membuat catatan NS delegasi `child.example.com` dengan empat server nama `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>`. Saat zona yang `child.example.com` dihosting dihapus tanpa menghapus catatan NS delegasi `example.com`, Route 53 melindungi `child.example.com` dari risiko catatan delegasi yang menggantung dengan mencegah `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>` agar tidak ditetapkan ke zona host yang baru dibuat dengan nama domain yang sama.

Skenario 2:

Mirip dengan skenario 1, tetapi kali ini Anda menghapus zona host anak DAN catatan NS delegasi di zona `example.com` yang dihosting. Namun, Anda menambahkan kembali catatan NS delegasi `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>` tanpa membuat zona host anak. Di sini `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>` menggantung catatan delegasi, karena Route 53 menghapus penahanan, yang mencegah `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>` ditetapkan dan sekarang akan memungkinkan zona host yang baru dibuat untuk menggunakan server nama di atas. Untuk mengurangi risiko, hapus `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>` dari catatan delegasi dan tambahkan kembali setelah zona host anak dibuat.

Skenario 3:

`<ns4>` Dalam skenario ini, Anda membuat set delegasi Route 53 yang dapat digunakan kembali dengan server nama `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>`. Kemudian, Anda mendelegasikan domain `example.com` ke server nama ini di domain induk `.com`. Namun, Anda belum membuat zona yang dihosting untuk `example.com` set delegasi yang dapat digunakan kembali. Di sini `<ns1>`, `<ns2>`, `<ns3>`, dan `<ns4>` menggantung catatan delegasi. `<ns2>`, `<ns3>`, dan `<ns4>` Untuk mengurangi risiko, buat zona yang dihosting menggunakan set delegasi yang dapat digunakan kembali dengan server nama `<ns1>`, dan `<ns4>`.

Identity and access management di Amazon Route 53

Untuk melakukan operasi apa pun di sumber daya Amazon Route 53, seperti mendaftarkan domain atau memperbarui catatan, AWS Identity and Access Management (IAM) mengharuskan Anda untuk mengautentikasi bahwa Anda adalah pengguna yang disetujui AWS. Jika Anda menggunakan konsol Route 53, Anda mengautentikasi identitas dengan memberikan nama pengguna dan kata sandi AWS Anda.

Setelah Anda mengautentikasi identitas Anda, IAM mengontrol akses Anda AWS dengan memverifikasi bahwa Anda memiliki izin untuk melakukan operasi dan mengakses sumber daya. Jika Anda adalah administrator akun, Anda dapat menggunakan IAM untuk mengontrol akses pengguna lain ke sumber daya yang terkait dengan akun Anda.

Bab ini menjelaskan cara menggunakan [IAM](#) dan Route 53 membantu mengamankan sumber daya Anda.

Topik

- [Mengautentikasi dengan identitas](#)
- [Kontrol akses](#)
- [Gambaran umum pengelolaan izin akses untuk sumber daya Amazon Route 53](#)
- [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Amazon Route 53](#)
- [Menggunakan Peran Tertaut Layanan untuk Amazon Route 53 Resolver](#)
- [AWS kebijakan terkelola untuk Amazon Route 53](#)
- [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#)
- [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#)

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 kredensi 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.

Kontrol akses

Untuk membuat, memperbarui, menghapus, atau membuat daftar sumber daya Amazon Route 53, Anda memerlukan izin untuk melakukan operasi, dan Anda memerlukan izin untuk mengakses sumber daya yang sesuai.

Bagian berikut menjelaskan cara mengelola izin untuk Route 53. Anda sebaiknya membaca gambaran umum terlebih dahulu.

Gambaran umum pengelolaan izin akses untuk sumber daya Amazon Route 53

Setiap AWS sumber daya dimiliki oleh AWS akun, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin.

Note

administrator akun (atau pengguna administrator) adalah pengguna yang memiliki hak istimewa administrator. Untuk informasi lebih lanjut tentang administrator, lihat [praktik terbaik IAM](#) dalam Panduan Pengguna IAM.

Ketika Anda memberikan izin, Anda memutuskan siapa yang mendapatkan izin, sumber daya yang mereka dapatkan izinnya, dan tindakan yang mereka dapatkan izinnya untuk tampil.

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. Konsol Manajemen AWS Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Disarankan) Gunakan kredensial konsol sebagai kredensial sementara untuk menandatangani permintaan terprogram ke,, atau. AWS CLI AWS SDKs AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk itu AWS CLI, lihat Login untuk pengembangan AWS lokal di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDKs, lihat Login untuk pengembangan AWS lokal di Panduan Referensi Alat AWS SDKs dan Alat.
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDKs, alat, dan AWS APIs, lihat Autentikasi Pusat Identitas IAM di Panduan Referensi Alat AWS SDKs dan Alat.
IAM	Gunakan kredensial sementara untuk menandatangani	Mengikuti petunjuk dalam Menggunakan kredensial

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
	permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensi jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensi pengguna IAM di Panduan Pengguna. AWS Command Line Interface • Untuk AWS SDKs dan alat, lihat Mengautentikasi menggunakan kredensi jangka panjang di Panduan Referensi Alat AWS SDKs dan Alat. • Untuk AWS APIs, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Topik

- [ARNs untuk sumber daya Amazon Route 53](#)
- [Memahami kepemilikan sumber daya](#)
- [Mengelola akses ke sumber daya](#)
- [Menentukan elemen kebijakan: Sumber daya, tindakan, efek, dan penanggung jawab](#)
- [Menentukan kondisi dalam kebijakan](#)

ARNs untuk sumber daya Amazon Route 53

Amazon Route 53 mendukung berbagai jenis sumber daya untuk DNS, pemeriksaan kondisi, dan pendaftaran domain. Dalam kebijakan, Anda dapat memberikan atau menolak akses ke sumber daya berikut dengan menggunakan * untuk ARN:

- Pemeriksaan kondisi
- Zona yang di-hosting
- Rangkaian delegasi yang dapat digunakan kembali
- Status kumpulan catatan sumber daya mengubah batch (hanya API)
- Kebijakan lalu lintas (arus lalu lintas)
- Instans kebijakan lalu lintas (arus lalu lintas)

Tidak semua sumber daya Route 53 mendukung izin. Anda tidak dapat memberikan atau menolak akses ke sumber daya berikut:

- Domain
- Catatan individu
- Tanda untuk domain
- Tanda untuk pemeriksaan kesehatan
- Tanda untuk zona yang di-host

Route 53 menyediakan tindakan API untuk bekerja dengan masing-masing jenis sumber daya ini. Untuk informasi lebih lanjut, lihat [Referensi API Amazon Route 53](#). Untuk daftar tindakan dan ARN yang Anda tetapkan untuk memberikan atau menolak izin penggunaan setiap tindakan, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

Memahami kepemilikan sumber daya

AWS Akun memiliki sumber daya yang dibuat di akun, terlepas dari siapa yang membuat sumber daya. Secara khusus, pemilik sumber daya adalah AWS akun entitas utama (yaitu, akun root, atau peran IAM) yang mengautentikasi permintaan pembuatan sumber daya.

Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensi akun root AWS akun Anda untuk membuat zona yang dihosting, AWS akun Anda adalah pemilik sumber daya.

- Jika Anda membuat pengguna di AWS akun Anda dan memberikan izin untuk membuat zona yang dihosting kepada pengguna tersebut, pengguna dapat membuat zona yang dihosting. Namun, akun AWS Anda yang dimiliki pengguna, memiliki sumber daya zona yang di-hosting.
- Jika Anda membuat peran IAM di AWS akun dengan izin untuk membuat zona yang dihosting, siapa pun yang dapat mengambil peran tersebut dapat membuat zona yang dihosting. AWS Akun Anda, tempat peran tersebut berada, memiliki sumber daya zona yang dihosting.

Mengelola akses ke sumber daya

Sebuah kebijakan izin menentukan siapa yang memiliki akses ke apa. Bagian ini menjelaskan opsi untuk membuat kebijakan izin untuk Amazon Route 53. Untuk informasi umum tentang sintaksis dan penjelasan kebijakan IAM, lihat [Referensi Kebijakan IAM AWS](#) dalam Panduan Pengguna IAM.

Kebijakan yang melekat pada identitas IAM disebut sebagai kebijakan berbasis identitas (IAM), dan kebijakan yang melekat pada sumber daya disebut sebagai kebijakan berbasis sumber daya. Route 53 hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Topik

- [Kebijakan berbasis identitas \(kebijakan IAM\)](#)
- [Kebijakan berbasis sumber daya](#)

Kebijakan berbasis identitas (kebijakan IAM)

Anda dapat melampirkan kebijakan ke identitas IAM Anda. Misalnya, Anda dapat melakukan hal berikut:

- Lampirkan kebijakan izin ke pengguna atau grup dalam akun Anda – Administrator akun dapat menggunakan kebijakan izin yang terkait dengan pengguna tertentu untuk memberikan izin bagi pengguna tersebut untuk membuat sumber daya Amazon Route 53.
- Lampirkan kebijakan izin ke peran (berikan izin lintas akun) — Anda dapat memberikan izin untuk melakukan tindakan Route 53 kepada pengguna yang dibuat oleh akun lain. AWS Untuk melakukannya, Anda melampirkan kebijakan izin pada IAM role, kemudian Anda mengizinkan pengguna di akun lain untuk menjalankan peran tersebut. Contoh berikut menjelaskan cara kerjanya untuk dua akun AWS, akun A dan B:
 1. Akun Administrator membuat IAM role dan melampirkan ke peran tersebut kebijakan izin yang memberikan izin untuk membuat atau mengakses sumber daya yang dimiliki oleh akun A.

2. Akun Administrator melampirkan kebijakan kepercayaan pada peran tersebut. Kebijakan kepercayaan mengidentifikasi akun B sebagai prinsipal yang dapat menjalankan peran tersebut.
3. Administrator Akun B kemudian dapat mendelegasikan izin untuk mengambil peran ke pengguna atau grup di akun B. Ini memungkinkan pengguna di akun B untuk membuat atau mengakses sumber daya di akun A.

Untuk informasi selengkapnya tentang cara mendelegasikan izin kepada pengguna di AWS akun lain, lihat [Manajemen akses di Panduan Pengguna IAM](#).

Kebijakan contoh berikut memungkinkan pengguna untuk melakukan tindakan `CreateHostedZone` untuk membuat zona yang di-hosting publik untuk setiap akun AWS :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone"
      ],
      "Resource": "*"
    }
  ]
}
```

Jika Anda ingin kebijakan juga berlaku untuk zona yang di-hosting pribadi, Anda perlu memberikan izin untuk menggunakan tindakan `AssociateVPCWithHostedZone` Route 53 dan dua tindakan Amazon EC2, `DescribeVpcs` dan `DescribeRegion`, seperti yang ditunjukkan dalam contoh berikut:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk informasi selengkapnya tentang melampirkan kebijakan pada identitas untuk Route 53, lihat [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Amazon Route 53](#). Untuk informasi lebih lanjut tentang pengguna, kelompok, peran, dan izin, lihat [Identitas \(Pengguna, Grup, dan Peran\)](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Layanan lain, seperti Amazon S3, juga support melampirkan kebijakan izin untuk sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. Amazon Route 53 tidak mendukung melampirkan kebijakan untuk sumber daya.

Menentukan elemen kebijakan: Sumber daya, tindakan, efek, dan penanggung jawab

Amazon Route 53 termasuk tindakan API (lihat [Referensi API Amazon Route 53](#)) yang dapat Anda gunakan pada setiap sumber daya Route 53 (lihat [ARNs untuk sumber daya Amazon Route 53](#)). Anda dapat memberikan pengguna atau izin pengguna gabungan untuk melakukan salah satu atau semua tindakan ini. Perhatikan bahwa beberapa tindakan API, seperti mendaftarkan domain, memerlukan izin untuk melakukan lebih dari satu tindakan.

Berikut ini adalah elemen-elemen kebijakan dasar:

- Sumber daya – Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang diberlakukan oleh kebijakan tersebut. Untuk informasi selengkapnya, lihat [ARNs untuk sumber daya Amazon Route 53](#).
- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak. Misalnya, tergantung pada Effect yang ditentukan, izin `route53:CreateHostedZone` memungkinkan atau menolak izin pengguna untuk melakukan tindakan `CreateHostedZone` Route 53.
- Efek – Anda menentukan efeknya, apakah mengizinkan atau menolak, ketika pengguna mencoba melakukan tindakan pada sumber daya tertentu. Jika Anda tidak secara eksplisit memberikan akses ke suatu tindakan, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun ada akses hibah kebijakan yang berbeda.
- Principal – Dalam kebijakan berbasis identitas (Kebijakan IAM), pengguna yang kebijakannya terlampir adalah principal yang implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang diinginkan untuk menerima izin (berlaku hanya untuk kebijakan berbasis sumber daya). Route 53 tidak mendukung kebijakan berbasis sumber daya.

Untuk informasi lebih lanjut tentang sintaksis dan deskripsi kebijakan IAM, lihat [AWS Referensi Kebijakan IAM](#) di Panduan Pengguna IAM.

Untuk daftar yang menampilkan semua operasi API Route 53 dan sumber daya yang mereka terapkan, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

Menentukan kondisi dalam kebijakan

Saat Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan IAM untuk menentukan kapan kebijakan harus berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan ketentuan dalam bahasa kebijakan, lihat [elemen kebijakan JSON IAM: Syarat](#) dalam Panduan Pengguna IAM.

Untuk menyatakan kondisi, Anda menggunakan kunci kondisi standar. Tidak ada tombol syarat khusus untuk Route 53. Namun, ada tombol kondisi AWS lebar yang dapat Anda gunakan sesuai kebutuhan. Untuk daftar lengkap tombol AWS lebar, lihat [Kunci yang tersedia untuk kondisi](#) di Panduan Pengguna IAM.

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk Amazon Route 53

Topik ini memberikan contoh kebijakan berbasis identitas yang menunjukkan cara administrator akun dapat melampirkan kebijakan izin ke identitas IAM dan dengan demikian memberikan izin untuk melakukan operasi di sumber daya Amazon Route 53.

Important

Kami menyarankan Anda untuk terlebih dahulu meninjau topik pendahuluan yang menjelaskan konsep dasar dan opsi untuk mengelola akses ke Route 53 sumber daya. Untuk informasi selengkapnya, lihat [Gambaran umum pengelolaan izin akses untuk sumber daya Amazon Route 53](#).

Note

Saat memberikan akses, zona yang dihosting dan VPC Amazon harus milik partisi yang sama. Partisi adalah sekelompok Wilayah AWS. Masing-masing Akun AWS dicakup ke satu partisi.

Berikut ini adalah partisi yang didukung:

- aws - Wilayah AWS
- aws-cn - Wilayah Tiongkok
- aws-us-gov - AWS GovCloud (US) Region

Untuk informasi selengkapnya, lihat [Access Management](#) dan [Amazon Route 53 endpoint dan kuota di Referensi AWS](#) Umum.

Topik

- [Izin diperlukan untuk menggunakan konsol Amazon Route 53](#)
- [Contoh izin untuk pemilik catatan domain](#)
- [Route 53 izin kunci terkelola pelanggan yang diperlukan untuk penandatanganan DNSSEC](#)
- [Contoh kebijakan yang dikelola pelanggan](#)

Contoh berikut menunjukkan kebijakan izin. Sid, atau ID pernyataan, adalah opsional:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPublicHostedZonePermissions",
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone",
        "route53:UpdateHostedZoneComment",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZonesByName"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowHealthCheckPermissions",
      "Effect": "Allow",
      "Action": [
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53>DeleteHealthCheck",
        "route53:GetCheckerIpRanges",
        "route53:GetHealthCheckCount",
        "route53:GetHealthCheckStatus",
        "route53:GetHealthCheckLastFailureReason"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan ini mencakup dua pernyataan:

- Pernyataan pertama memberikan izin untuk tindakan yang diperlukan untuk membuat dan mengelola zona yang di-hosting publik dan catatan mereka. Karakter wildcard (*) di Amazon Resource Name (ARN) memberikan akses ke semua zona host yang dimiliki oleh akun saat ini. AWS
- Pernyataan kedua memberikan izin untuk semua tindakan yang diperlukan untuk membuat dan mengelola pemeriksaan kondisi.

Untuk daftar tindakan dan ARN yang Anda tetapkan untuk memberikan atau menolak izin penggunaan setiap tindakan, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

Izin diperlukan untuk menggunakan konsol Amazon Route 53

Untuk memberikan akses penuh ke Amazon Route 53 Anda memberikan izin dalam kebijakan izin berikut:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:*",
        "route53domains:*",
        "tag:*",
        "ssm:GetParametersByPath",
        "cloudfront:ListDistributions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```



```

        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:ModifyNetworkInterfaceAttribute",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:CreateTopic",
        "kms:ListAliases",
        "kms:DescribeKey",
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:Sign",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricStatistics"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": "arn:aws:apigateway:*::/domainnames"
  }
]
}

```

Inilah mengapa izin diperlukan:

route53:*

Memungkinkan Anda melakukan semua tindakan Route 53 kecuali hal berikut:

- Membuat dan memperbarui catatan alias yang nilai Alias Target adalah CloudFront distribusi, penyeimbang beban Elastic Load Balancing, lingkungan Elastic Beanstalk, atau bucket Amazon S3. (Dengan izin ini, Anda dapat membuat catatan alias yang nilai Target Alias adalah catatan lain di zona yang di-hosting yang sama.)
- Bekerja dengan zona pribadi yang di-hosting.
- Bekerja dengan domain.

- Buat, hapus, dan lihat CloudWatch alarm.
- Render CloudWatch metrik di konsol Route 53.

route53domains:*

Memungkinkan Anda bekerja dengan domain.

Important

Jika Anda membuat daftar tindakan `route53` secara individual, Anda harus memasukkan `route53:CreateHostedZone` untuk bekerja dengan domain. Ketika Anda mendaftar domain, zona yang di-hosting dibuat pada saat yang sama, sehingga kebijakan yang mencakup izin untuk mendaftar domain juga memerlukan izin untuk membuat zona yang di-hosting.

Untuk pendaftaran domain, Route 53 tidak mendukung pemberian atau menolak izin untuk sumber daya individu.

route53resolver:*

Memungkinkan Anda bekerja dengan Route 53 VPC Resolver.

ssm:GetParametersByPath

Memungkinkan Anda mengambil Wilayah yang tersedia untuk umum saat Anda membuat catatan alias baru, zona yang dihosting pribadi, dan pemeriksaan kesehatan.

cloudfront:ListDistributions

Memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Alias Target adalah CloudFront distribusi.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan daftar distribusi untuk ditampilkan di konsol.

elasticloadbalancing:DescribeLoadBalancers

Memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Target Alias adalah penyeimbang beban ELB.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan daftar penyeimbang beban untuk ditampilkan di konsol.

elasticbeanstalk:DescribeEnvironments

Memungkinkan Anda membuat dan memperbarui catatan alias ketika nilai Target Alias adalah lingkungan Elastic Beanstalk.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan daftar lingkungan untuk ditampilkan di konsol.

s3:ListAllMyBuckets, s3:GetBucketLocation, dan s3:GetBucketWebsite

Memungkinkan Anda membuat dan memperbarui catatan alias di mana nilai Target Alias adalah bucket Amazon S3. (Anda dapat membuat alias ke bucket Amazon S3 hanya jika bucket dikonfigurasi sebagai titik akhir situs web; `s3:GetBucketWebsite` mendapatkan informasi konfigurasi yang diperlukan.)

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan daftar bucket untuk ditampilkan di konsol.

ec2:DescribeVpcs dan ec2:DescribeRegions

Memungkinkan Anda bekerja dengan pribadi yang di-hosting.

Semua **ec2** terdaftar

Biarkan Anda bekerja dengan Route 53 VPC Resolver.

sns:ListTopics, sns:ListSubscriptionsByTopic, sns:CreateTopic, cloudwatch:DescribeAlarms, cloudwatch:PutMetricAlarm, cloudwatch>DeleteAlarms

Memungkinkan Anda membuat, menghapus, dan melihat CloudWatch alarm.

cloudwatch:GetMetricStatistics

Memungkinkan Anda membuat pemeriksaan kesehatan CloudWatch metrik.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan statistik untuk ditampilkan di konsol.

apigateway:GET

Memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Target Alias adalah API Amazon API Gateway.

Izin ini tidak diperlukan jika Anda tidak menggunakan konsol Route 53. Route 53 menggunakannya hanya untuk mendapatkan daftar APIs untuk ditampilkan di konsol.

kms : *

Memungkinkan Anda bekerja sama AWS KMS untuk mengaktifkan penandatanganan DNSSEC.

Contoh izin untuk pemilik catatan domain

Dengan izin kumpulan catatan sumber daya, Anda dapat mengatur izin terperinci yang membatasi apa yang dapat diperbarui atau AWS dimodifikasi pengguna. Untuk informasi selengkapnya, lihat [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#).

Dalam beberapa skenario, pemilik zona yang di-hosting mungkin bertanggung jawab untuk manajemen keseluruhan zona yang di-hosting, sementara orang lain dalam organisasi bertanggung jawab untuk subset dari tugas-tugas tersebut. Pemilik zona yang dihosting yang telah mengaktifkan penandatanganan DNSSEC, misalnya, mungkin ingin membuat kebijakan IAM yang menyertakan izin bagi orang lain untuk menambah dan menghapus Resource Set Records (RRs) di zona yang dihosting, di antara tugas-tugas lainnya. Izin khusus yang dipilih pemilik zona yang di-hosting untuk mengaktifkan pemilik catatan atau orang lain akan bergantung pada kebijakan organisasi mereka.

Berikut ini adalah contoh kebijakan IAM yang memungkinkan pemilik catatan untuk melakukan modifikasi, kebijakan lalu lintas RRs, dan pemeriksaan kesehatan. Pemilik rekaman dengan kebijakan ini tidak diperbolehkan untuk melakukan operasi tingkat zona, seperti membuat atau menghapus zona, mengaktifkan atau menonaktifkan permintaan pembuatan log, membuat atau menghapus kumpulan delegasi dapat digunakan kembali, atau mengubah pengaturan DNSSEC.

```
{
  "Sid": "Do not allow zone-level modification ",
  "Effect": "Allow",
  "Action": [
    "route53:ChangeResourceRecordSets",
    "route53:CreateTrafficPolicy",
    "route53>DeleteTrafficPolicy",
    "route53:CreateTrafficPolicyInstance",
    "route53:CreateTrafficPolicyVersion",
    "route53:UpdateTrafficPolicyInstance",
    "route53:UpdateTrafficPolicyComment",
    "route53>DeleteTrafficPolicyInstance",
    "route53:CreateHealthCheck",
    "route53:UpdateHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:List*",
  ]
}
```

```

    "route53:Get*"
  ],
  "Resource": [
    "*"
  ]
}

```

Route 53 izin kunci terkelola pelanggan yang diperlukan untuk penandatanganan DNSSEC

Saat Anda mengaktifkan penandatanganan DNSSEC untuk Route 53, Route 53 membuat kunci penandatanganan kunci (KSK) berdasarkan kunci yang dikelola pelanggan di (). AWS Key Management Service AWS KMS Anda dapat menggunakan kunci terkelola pelanggan yang sudah ada yang mendukung penandatanganan DNSSEC atau membuat yang baru. Route 53 harus memiliki izin untuk mengakses kunci yang dikelola pelanggan Anda sehingga dapat membuat KSK untuk Anda.

Untuk mengaktifkan Route 53 mengakses kunci terkelola pelanggan Anda, pastikan kebijakan kunci terkelola pelanggan Anda berisi pernyataan berikut:

```

{
  "Sid": "Allow Route 53 DNSSEC Service",
  "Effect": "Allow",
  "Principal": {
    "Service": "dnssec-route53.amazonaws.com"
  },
  "Action": ["kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:Sign"],
  "Resource": "*"
},
{
  "Sid": "Allow Route 53 DNSSEC to CreateGrant",
  "Effect": "Allow",
  "Principal": {
    "Service": "dnssec-route53.amazonaws.com"
  },
  "Action": ["kms:CreateGrant"],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}

```

```

    }
  }
}

```

Masalah deputy yang membingungkan adalah masalah keamanan di mana entitas tanpa izin untuk suatu tindakan dapat memaksa entitas yang lebih istimewa untuk melakukannya. Untuk melindungi Anda AWS KMS dari itu, Anda dapat secara opsional membatasi izin yang dimiliki layanan ke sumber daya dalam kebijakan berbasis sumber daya dengan menyediakan kombinasi `aws:SourceAccount` dan `aws:SourceArn` ketentuan (keduanya atau satu). `aws:SourceAccount` adalah ID AWS akun pemilik zona yang dihosting. `aws:SourceArn` adalah ARN dari zona yang dihosting.

Berikut ini adalah dua contoh izin yang dapat Anda tambahkan:

```

{
  "Sid": "Allow Route 53 DNSSEC Service",
  ...
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    },
    "ArnEquals": {
      "aws:SourceArn": "arn:aws:route53::hostedzone/HOSTED_ZONE_ID"
    }
  }
},

```

- Atau -

```

{
  "Sid": "Allow Route 53 DNSSEC Service",
  ...
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": ["1111-2222-3333", "4444-5555-6666"]
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:route53::hostedzone/*"
    }
  }
}

```

```
},
```

Untuk informasi selengkapnya, lihat [Masalah confused deputy](#) di Panduan Pengguna IAM.

Contoh kebijakan yang dikelola pelanggan

Anda dapat membuat kebijakan IAM khusus untuk mengizinkan izin tindakan Route 53. Anda dapat melampirkan kebijakan khusus ini ke grup IAM yang memerlukan izin yang ditentukan. Kebijakan ini berfungsi saat Anda menggunakan API Route 53, CLI AWS SDKs, atau AWS CLI. Contoh-contoh berikut menunjukkan izin untuk beberapa kasus penggunaan umum. Untuk kebijakan yang memberi pengguna akses penuh ke Route 53, lihat [Izin diperlukan untuk menggunakan konsol Amazon Route 53](#).

Contoh

- [Contoh 1: Memungkinkan akses baca ke semua zona yang di-hosting](#)
- [Contoh 2: Memungkinkan pembuatan dan penghapusan zona yang di-hosting](#)
- [Contoh 3: Memungkinkan akses penuh ke semua domain \(zona yang di-hosting publik saja\)](#)
- [Contoh 4: Izinkan pembuatan titik akhir Route 53 VPC Resolver masuk dan keluar](#)

Contoh 1: Memungkinkan akses baca ke semua zona yang di-hosting

Kebijakan izin berikut memberikan izin pengguna untuk membuat daftar semua zona yang di-hosting dan melihat semua catatan di zona yang di-hosting.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource": "*"
    },
    {
```

```

        "Effect": "Allow",
        "Action": ["route53:ListHostedZones"],
        "Resource": "*"
    }
]
}

```

Contoh 2: Memungkinkan pembuatan dan penghapusan zona yang di-hosting

Kebijakan izin berikut memungkinkan pengguna untuk membuat dan menghapus zona yang di-hosting, dan melacak kemajuan perubahan.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["route53:CreateHostedZone"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["route53>DeleteHostedZone"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["route53:GetChange"],
      "Resource": "*"
    }
  ]
}

```

Contoh 3: Memungkinkan akses penuh ke semua domain (zona yang di-hosting publik saja)

Kebijakan izin berikut memungkinkan pengguna untuk melakukan semua tindakan pada pendaftaran domain, termasuk izin untuk mendaftarkan domain dan membuat zona yang di-hosting.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53domains:*",
        "route53:CreateHostedZone"
      ],
      "Resource": "*"
    }
  ]
}
```

Ketika Anda mendaftar domain, zona yang di-hosting dibuat pada saat yang sama, sehingga kebijakan yang mencakup izin untuk mendaftar domain juga memerlukan izin untuk membuat zona yang di-hosting. (Untuk pendaftaran domain, Route 53 tidak mendukung pemberian izin untuk sumber daya individu.)

Untuk informasi tentang izin yang diperlukan untuk bekerja dengan zona yang di-hosting pribadi, lihat [Izin diperlukan untuk menggunakan konsol Amazon Route 53](#).

Contoh 4: Izinkan pembuatan titik akhir Route 53 VPC Resolver masuk dan keluar

Kebijakan izin berikut memungkinkan pengguna untuk menggunakan konsol Route 53 untuk membuat titik akhir Resolver inbound dan outbound.

Beberapa izin ini diperlukan hanya untuk membuat titik akhir di konsol. Anda dapat menghilangkan izin ini jika Anda ingin memberikan izin hanya untuk membuat titik akhir inbound dan outbound secara terprogram:

- `route53resolver:ListResolverEndpoints` memungkinkan pengguna melihat daftar titik akhir inbound atau outbound sehingga mereka dapat memverifikasi bahwa titik akhir telah dibuat.
- `DescribeAvailabilityZones` diperlukan untuk menampilkan daftar Availability Zone.
- `DescribeVpcs` diperlukan untuk menampilkan daftar VPCs.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "route53resolver:CreateResolverEndpoint",
        "route53resolver:ListResolverEndpoints",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    }
  ]
}
```

Menggunakan Peran Tertaut Layanan untuk Amazon Route 53 Resolver

[Route 53 VPC Resolver menggunakan peran terkait layanan AWS Identity and Access Management \(IAM\)](#). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke VPC Resolver. Peran terkait layanan telah ditentukan sebelumnya oleh VPC Resolver dan mencakup semua izin yang diperlukan layanan untuk memanggil layanan lain atas nama Anda. AWS

Peran terkait layanan membuat pengaturan Resolver VPC lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. VPC Resolver mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya VPC Resolver yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Resolver VPC Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [Layanan AWS yang Bekerja Bersama IAM](#) dan mencari layanan yang memuat Ya dalam kolom Peran yang Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

- [Izin Peran Tertaut Layanan untuk Resolver VPC](#)
- [Membuat Peran Tertaut Layanan untuk VPC Resolver](#)
- [Mengedit Peran Tertaut Layanan untuk Resolver VPC](#)
- [Menghapus Peran Tertaut Layanan untuk VPC Resolver](#)
- [Wilayah yang Didukung untuk Peran Tertaut Layanan Resolver VPC](#)

Izin Peran Tertaut Layanan untuk Resolver VPC

VPC Resolver menggunakan peran **AWSServiceRoleForRoute53Resolver** terkait layanan untuk mengirimkan log kueri atas nama Anda.

Kebijakan izin peran memungkinkan VPC Resolver menyelesaikan tindakan berikut pada sumber daya Anda:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
}  
]  
}
```

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat [Izin Peran Tertaut Layanan](#) di Panduan Pengguna IAM.

Membuat Peran Tertaut Layanan untuk VPC Resolver

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat asosiasi konfigurasi log kueri resolver di konsol Amazon Route 53, atau AWS API AWS CLI, VPC Resolver akan membuat peran terkait layanan untuk Anda.

Important

Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Juga, jika Anda menggunakan layanan VPC Resolver sebelum 12 Agustus 2020, ketika mulai mendukung peran terkait layanan, maka VPC Resolver membuat peran di akun Anda.

`AWSServiceRoleForRoute53Resolver` Untuk mempelajari lebih lanjut, lihat [Peran Baru yang Muncul di Akun IAM Saya](#).

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat asosiasi konfigurasi log kueri Resolver baru, peran `AWSServiceRoleForRoute53Resolver` terkait layanan akan dibuat untuk Anda lagi.

Mengedit Peran Tertaut Layanan untuk Resolver VPC

VPC Resolver tidak memungkinkan Anda untuk mengedit peran terkait layanan.

`AWSServiceRoleForRoute53Resolver` Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit Peran Tertaut Layanan](#) dalam Panduan Pengguna IAM.

Menghapus Peran Tertaut Layanan untuk VPC Resolver

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

Note

Jika layanan VPC Resolver menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya VPC Resolver yang digunakan oleh

AWSServiceRoleForRoute53Resolver

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Memperluas menu konsol Route 53. Di sudut kiri atas konsol, pilih ikon tiga bilah horizontal ().
3. Dalam menu Resolver (Resolver), pilih Query logging (Pencatatan kueri).
4. Pilih kotak centang di samping nama konfigurasi pembuatan log kueri Anda, lalu pilih Delete (Hapus).
5. Di kotak teks Delete query logging configuration (Hapus konfigurasi pembuatan log kueri), pilih Stop logging queries (Berhenti membuat log kueri).

Ini akan memisahkan konfigurasi dari VPC. Anda juga dapat memisahkan konfigurasi pembuatan log kueri secara terprogram. Untuk informasi selengkapnya, lihat [disassociate-resolver-query-log-config](#).

6. Setelah pembuatan log kueri telah berhenti, Anda dapat secara opsional mengetik **delete** pada bidang, dan pilih Delete (Hapus) untuk menghapus konfigurasi pembuatan log kueri. Namun, ini tidak diperlukan untuk menghapus sumber daya yang digunakan oleh **AWSServiceRoleForRoute53Resolver**.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForRoute53Resolver` terkait layanan. Untuk informasi selengkapnya, silakan lihat [Menghapus Peran Terkait Layanan](#) di Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Tertaut Layanan Resolver VPC

VPC Resolver tidak mendukung penggunaan peran terkait layanan di setiap Wilayah tempat layanan tersedia. Anda dapat menggunakan `AWSServiceRoleForRoute53Resolver` peran di Wilayah berikut.

Nama wilayah	Identitas wilayah	Support di VPC Resolver
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Canada (Central)	ca-sentral-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya
Europe (Paris)	eu-west-3	Ya

Nama wilayah	Identitas wilayah	Support di VPC Resolver
South America (São Paulo)	sa-east-1	Ya
China (Beijing)	cn-north-1	Ya
Tiongkok (Ningxia)	cn-northwest-1	Ya
AWS GovCloud (US)	us-gov-east-1	Ya
AWS GovCloud (US)	us-gov-west-1	Ya

AWS kebijakan terkelola untuk Amazon Route 53

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, pembaruan 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 kebijakan terkelola: AmazonRoute 53 FullAccess

Anda dapat melampirkan kebijakan AmazonRoute53FullAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses penuh ke sumber daya Route 53, termasuk pendaftaran domain dan pemeriksaan kesehatan, tetapi tidak termasuk Resolver VPC.

Detail izin

Kebijakan ini mencakup izin berikut.

- `route53:*` – Memungkinkan Anda melakukan semua tindakan Route 53 kecuali berikut:
 - Membuat dan memperbarui catatan alias yang nilai Alias Target adalah CloudFront distribusi, penyeimbang beban Elastic Load Balancing, lingkungan Elastic Beanstalk, atau bucket Amazon S3. (Dengan izin ini, Anda dapat membuat catatan alias yang nilai Target Alias adalah catatan lain di zona yang di-hosting yang sama.)
 - Bekerja dengan zona pribadi yang di-hosting.
 - Bekerja dengan domain.
 - Buat, hapus, dan lihat CloudWatch alarm.
 - Render CloudWatch metrik di konsol Route 53.
- `route53domains:*`— Memungkinkan Anda bekerja dengan domain.
- `cloudfront:ListDistributions`— Memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Alias Target adalah CloudFront distribusi.

Izin ini tidak diperlukan jika Anda tidak menggunakan konsol Route 53. Route 53 menggunakannya hanya untuk mendapatkan daftar distribusi untuk ditampilkan di konsol.

- `cloudfront:GetDistributionTenantByDomain`— Digunakan untuk mengambil distribusi CloudFront multi-penyewa untuk memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Alias Target adalah penyewa distribusi. CloudFront
- `cloudfront:GetConnectionGroup`— Digunakan untuk mengambil distribusi CloudFront multi-penyewa untuk memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Alias Target adalah penyewa distribusi. CloudFront
- `cloudwatch:DescribeAlarms`— Bersama dengan `sns:ListTopics` dan `sns:ListSubscriptionsByTopic`, memungkinkan Anda membuat, menghapus, dan melihat CloudWatch alarm.
- `cloudwatch:GetMetricStatistics`— Memungkinkan Anda membuat pemeriksaan kesehatan CloudWatch metrik.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan statistik untuk ditampilkan di konsol.

- `cloudwatch:GetMetricData`— Memungkinkan Anda menampilkan status metrik pemeriksaan CloudWatch kesehatan Anda.
- `ec2:DescribeVpcs`— Memungkinkan Anda menampilkan daftar VPCs.
- `ec2:DescribeVpcEndpoints` — Memungkinkan Anda menampilkan daftar VPC endpoint.

- `ec2:DescribeRegions` — Memungkinkan Anda menampilkan daftar Availability Zone.
- `elasticloadbalancing:DescribeLoadBalancers`— Memungkinkan Anda membuat dan memperbarui catatan alias di mana nilai Target Alias adalah penyeimbang beban Elastic Load Balancing.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan daftar penyeimbang beban untuk ditampilkan di konsol.

- `elasticbeanstalk:DescribeEnvironments`— Memungkinkan Anda membuat dan memperbarui catatan alias di mana nilai Target Alias adalah lingkungan Elastic Beanstalk.

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakannya hanya untuk mendapatkan daftar lingkungan untuk ditampilkan di konsol.

- `es:ListDomainNames`— Memungkinkan Anda menampilkan nama semua domain OpenSearch Layanan Amazon yang dimiliki oleh pengguna saat ini di Wilayah aktif.
- `es:DescribeDomains`— Memungkinkan Anda mendapatkan konfigurasi domain untuk domain OpenSearch Layanan Amazon yang ditentukan.
- `lightsail:GetContainerServices`— Memungkinkan Anda layanan kontainer Lightsail untuk memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Alias Target adalah domain Lightsail.
- `s3:ListBucket`, `s3:GetBucketLocation`, dan `s3:GetBucketWebsite`— Memungkinkan Anda membuat dan memperbarui catatan alias di mana nilai Target Alias adalah bucket Amazon S3. (Anda dapat membuat alias ke bucket Amazon S3 hanya jika bucket dikonfigurasi sebagai titik akhir situs web; `s3:GetBucketWebsite` mendapatkan informasi konfigurasi yang diperlukan.)

Izin ini tidak diperlukan jika Anda tidak menggunakan Route 53 konsol. Route 53 menggunakan ini hanya untuk mendapatkan daftar bucket untuk ditampilkan di konsol.

- `sns:ListTopics`, `sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Memungkinkan Anda membuat, menghapus, dan melihat CloudWatch alarm.
- `tag:GetResources`— Memungkinkan Anda menampilkan tag di sumber daya Anda. Misalnya, nama-nama pemeriksaan kesehatan Anda.
- `apigateway:GET` – Memungkinkan Anda membuat dan memperbarui catatan alias yang nilai Target Alias adalah API Amazon API Gateway.

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "apigateway:GET",
      "Resource": "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

AWS kebijakan terkelola: AmazonRoute 53 ReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonRoute53ReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses hanya-baca ke sumber daya Route 53, termasuk pendaftaran domain dan pemeriksaan kesehatan, tetapi tidak termasuk Resolver VPC.

Detail izin

Kebijakan ini mencakup izin berikut.

- `route53:Get*` — Mendapatkan sumber daya Route 53.
- `route53:List*` — Daftar sumber daya Route 53.
- `route53:TestDNSAnswer` — Mendapatkan nilai yang dihasilkan Route 53 dalam menanggapi permintaan DNS.

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS kebijakan terkelola: AmazonRoute 53 DomainsFullAccess

Anda dapat melampirkan kebijakan AmazonRoute53DomainsFullAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses penuh ke sumber daya pendaftaran domain Route 53.

Detail izin

Kebijakan ini mencakup izin berikut.

- `route53:CreateHostedZone` – Memungkinkan Anda membuat zona yang di-hosting Route 53.
- `route53domains:*` – Memungkinkan Anda mendaftarkan nama domain dan melakukan operasi terkait.

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS kebijakan terkelola: AmazonRoute 53 DomainsReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonRoute53DomainsReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses hanya-baca ke Route 53 pendaftaran domain.

Detail izin

Kebijakan ini mencakup izin berikut.

- `route53domains:Get*` — Memungkinkan Anda mengambil daftar domain dari Route 53.
- `route53domains:List*` — Memungkinkan Anda menampilkan daftar domain Route 53.

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS kebijakan terkelola: AmazonRoute 53 ResolverFullAccess

Anda dapat melampirkan kebijakan AmazonRoute53ResolverFullAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses penuh ke sumber daya Resolver VPC Route 53.

Detail izin

Kebijakan ini mencakup izin berikut.

- `route53resolver:*`— Memungkinkan Anda membuat dan mengelola sumber daya Resolver VPC di konsol Route 53.
- `ec2:DescribeSubnets` – Memungkinkan Anda mencantumkan subnet Amazon VPC Anda.
- `ec2:CreateNetworkInterface`, `ec2>DeleteNetworkInterface`, dan `ec2:ModifyNetworkInterfaceAttribute` – Memungkinkan Anda membuat, memodifikasi, dan menghapus antarmuka jaringan.
- `ec2:DescribeNetworkInterfaces` – Memungkinkan Anda menampilkan daftar antarmuka jaringan.
- `ec2:DescribeSecurityGroups` – Memungkinkan Anda menampilkan daftar semua grup keamanan Anda.
- `ec2:DescribeVpcs`— Memungkinkan Anda menampilkan daftar VPCs.
- `ec2:DescribeAvailabilityZones` – Memungkinkan Anda mencantumkan zona yang tersedia untuk Anda.

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ResolverFullAccess",
      "Effect": "Allow",
      "Action": [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": [
```

```

    "": [
      {
        "": [
          {
            "": "*"
          }
        ]
      }
    ]
  }
}

```

AWS kebijakan terkelola: AmazonRoute 53 ResolverReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonRoute53ResolverReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses hanya-baca ke sumber daya Resolver VPC Route 53.

Detail izin

Kebijakan ini mencakup izin berikut.

- `route53resolver:Get*`— Mendapat sumber daya VPC Resolver.
- `route53resolver:List*`— Memungkinkan Anda menampilkan daftar sumber daya VPC Resolver.
- `ec2:DescribeNetworkInterfaces` – Memungkinkan Anda menampilkan daftar antarmuka jaringan.
- `ec2:DescribeSecurityGroups` – Memungkinkan Anda menampilkan daftar semua grup keamanan Anda.

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ResolverReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "route53resolver:Get*",

```

```

        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

AWS kebijakan terkelola: Route53 ResolverServiceRolePolicy

Anda tidak dapat melampirkan Route53ResolverServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Resolver VPC Route 53 mengakses AWS layanan dan sumber daya yang digunakan atau dikelola oleh VPC Resolver. Untuk informasi selengkapnya, lihat [Menggunakan Peran Tertaut Layanan untuk Amazon Route 53 Resolver](#).

AWS kebijakan terkelola: AmazonRoute 53 ProfilesFullAccess

Anda dapat melampirkan kebijakan AmazonRoute53ProfilesReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses penuh ke sumber daya Profil Amazon Route 53.

Detail izin

Kebijakan ini mencakup izin berikut.

- route53profiles— Memungkinkan Anda membuat dan mengelola sumber daya Profil di konsol Route 53.
- ec2— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang VPCs

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ProfilesFullAccess",
      "Effect": "Allow",
      "Action": [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles>DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:PutProfilePolicy",
        "route53profiles:ListTagsForResource",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS kebijakan terkelola: AmazonRoute 53 ProfilesReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonRoute53ProfilesReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses hanya-baca ke sumber daya Profil Amazon Route 53.

Detail izin

Untuk informasi selengkapnya tentang izin, lihat [Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Rute pembaruan 53 ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Route 53 sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di [halaman Riwayat dokumen](#) Route 53.

Ubah	Deskripsi	Date
AmazonRoute53 FullAccess - Kebijakan yang diperbarui	Menambahkan izin untuk <code>cloudwatch:GetMetricData</code> , <code>tag:GetResources</code> , <code>es:ListDomainNames</code> , <code>es:DescribeDomains</code> , <code>cloudfront:GetDistributionTextByDomain</code> , <code>cloudfront:GetConnectionGroup</code> dan <code>lightsail:GetContainerServices</code> . Izin ini memungkinkan Anda mengambil hingga 500 metrik pemeriksaan CloudWatch kesehatan, hingga 100 nama pemeriksaan kesehatan, mendapatkan konfigurasi domain untuk domain Layanan Amazon yang ditentukan, dan mencantumkan nama semua domain OpenSearch Layanan Amazon yang dimiliki oleh pengguna saat ini di Wilayah aktif, ambil distribusi CloudFront multi-penyewa,	01 Juni 2025

Ubah	Deskripsi	Date
	dan dapatkan OpenSearch layanan kontainer Lightsail.	
AmazonRoute53 ProfilesFullAccess - Kebijakan yang diperbarui	Menambahkan izin untuk <code>GetProfilePolicy</code> dan <code>PutProfilePolicy</code> . Ini adalah tindakan IAM khusus izin. Jika kepala sekolah IAM tidak memiliki izin ini diberikan , kesalahan akan terjadi saat mencoba membagikan Profil menggunakan layanan. AWS RAM	Agustus 27, 2024
AmazonRoute53 ProfilesReadOnlyAccess - Kebijakan yang diperbarui	Menambahkan izin untuk <code>GetProfilePolicy</code> . Ini adalah tindakan IAM khusus izin. Jika kepala sekolah IAM tidak memiliki izin ini diberikan, kesalahan akan terjadi saat mencoba mengakses kebijakan Profil menggunakan layanan. AWS RAM	Agustus 27, 2024
AmazonRoute53 ResolverFullAccess - Kebijakan yang diperbarui	Menambahkan id pernyataan (Sid) untuk mengidentifikasi kebijakan secara unik.	Agustus 5, 2024
AmazonRoute53 ResolverReadOnlyAccess - Kebijakan yang diperbarui	Menambahkan id pernyataan (Sid) untuk mengidentifikasi kebijakan secara unik.	Agustus 5, 2024

Ubah	Deskripsi	Date
AmazonRoute53 ProfilesFullAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses penuh ke sumber daya Profil Amazon Route 53.	April 22, 2024
AmazonRoute53 ProfilesReadOnlyAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses hanya-baca ke sumber daya Profil Amazon Route 53.	April 22, 2024
Route53 ResolverServiceRolePolicy - Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru yang dilampirkan ke peran terkait layanan yang memungkinkan VPC Resolver mengakses AWS layanan dan sumber daya yang digunakan atau dikelola oleh Resolver.	14 Juli 2021
AmazonRoute53 ResolverReadOnlyAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses hanya-baca ke sumber daya Resolver VPC.	14 Juli 2021
AmazonRoute53 ResolverFullAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses penuh ke sumber daya VPC Resolver.	14 Juli 2021

Ubah	Deskripsi	Date
AmazonRoute53 DomainsReadOnlyAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses hanya-baca ke sumber daya domain Route 53.	14 Juli 2021
AmazonRoute53 DomainsFullAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses penuh ke sumber daya domain Route 53.	14 Juli 2021
AmazonRoute53 ReadOnlyAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk mengizinkan akses hanya-baca ke sumber daya Route 53.	14 Juli 2021
AmazonRoute53 FullAccess — Kebijakan baru	Amazon Route 53 menambahkan kebijakan baru untuk memungkinkan akses penuh ke sumber daya Route 53.	14 Juli 2021
Route 53 mulai melacak perubahan	Route 53 mulai melacak perubahan untuk kebijakan yang AWS dikelola.	14 Juli 2021

Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci

Di Route 53, Anda dapat menentukan kondisi saat memberikan izin menggunakan kebijakan IAM (lihat). [Kontrol akses](#) Sebagai contoh, Anda dapat:

- Berikan izin untuk mengizinkan akses ke satu set catatan sumber daya.

- Berikan izin untuk memungkinkan pengguna mengakses semua kumpulan rekaman sumber daya dari jenis catatan DNS tertentu di zona yang dihosting, misalnya catatan A dan AAAA.
- Berikan izin untuk memungkinkan pengguna mengakses kumpulan catatan sumber daya di mana namanya berisi string tertentu.
- Berikan izin untuk mengizinkan pengguna hanya melakukan sebagian CREATE | UPSERT | DELETE tindakan di konsol Route 53, atau saat menggunakan API. [ChangeResourceRecordSets](#)
- Berikan izin untuk memungkinkan pengguna mengaitkan atau memisahkan zona host pribadi dari VPC tertentu.
- Berikan izin untuk memungkinkan pengguna mencantumkan zona yang dihosting yang terkait dengan VPC tertentu.
- Berikan izin untuk memungkinkan pengguna mengakses untuk membuat zona host pribadi baru dan mengaitkannya ke VPC tertentu.
- Berikan izin untuk memungkinkan pengguna membuat atau menghapus otorisasi asosiasi VPC.

Anda juga dapat membuat izin yang menggabungkan izin granular apa pun.

Menormalkan nilai kunci kondisi Route 53

Nilai yang Anda masukkan untuk kondisi kebijakan harus diformat, atau dinormalisasi, sebagai berikut:

Untuk **route53:ChangeResourceRecordSetsNormalizedRecordNames**:

- Semua huruf harus huruf kecil.
- Nama DNS harus tanpa trailing dot.
- Karakter selain a—z, 0—9, - (tanda hubung), _ (garis bawah), dan . (periode, sebagai pembatas antara label) harus menggunakan kode escape dalam format \ kode oktal tiga digit. Misalnya, \052 adalah kode oktal untuk karakter*.

Untuk **route53:ChangeResourceRecordSetsActions**, nilainya dapat berupa salah satu dari yang berikut dan harus huruf besar:

- CREATE
- MENEGAKKAN
- DELETE

Untuk **route53:ChangeResourceRecordSetsRecordTypes**:

- Nilai harus dalam huruf besar, dan dapat berupa salah satu jenis catatan DNS yang didukung Route 53. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Untuk **route53:VPCs**:

- Nilai harus dalam format `VPCId=<vpc-id>,VPCRegion=<region>`.
- Nilai `<vpc-id>` dan `<region>` harus dalam huruf kecil, seperti `VPCId=vpc-123abc` dan `VPCRegion=us-east-1`.
- Kunci konteks dan nilai peka huruf besar/kecil.

Important

Agar izin Anda mengizinkan atau membatasi tindakan sesuai keinginan, Anda harus mengikuti konvensi ini. Hanya VPCId dan VPCRegion elemen yang diterima oleh kunci kondisi ini, AWS sumber daya lainnya, seperti Akun AWS, tidak didukung.

Anda dapat menggunakan [Access Analyzer](#) atau [Policy Simulator](#) di Panduan Pengguna IAM untuk memvalidasi bahwa kebijakan Anda memberikan atau membatasi izin seperti yang diharapkan. Anda juga dapat memvalidasi izin dengan menerapkan kebijakan IAM ke pengguna pengujian atau peran untuk menjalankan operasi Route 53.

Menentukan kondisi: menggunakan tombol kondisi

AWS menyediakan satu set kunci kondisi yang telah ditentukan (AWS-wide condition keys) untuk semua AWS layanan yang mendukung IAM untuk kontrol akses. Misalnya, Anda dapat menggunakan kunci kondisi `aws:SourceIp` untuk memeriksa alamat IP pemohon sebelum mengizinkan tindakan yang akan dilakukan. Untuk informasi selengkapnya dan daftar tombol AWS-wide, lihat [Kunci Tersedia untuk Ketentuan](#) di Panduan Pengguna IAM.

Note

Route 53 tidak mendukung kunci kondisi berbasis tag.

Tabel berikut menunjukkan kunci kondisi khusus layanan Route 53 yang berlaku untuk Route 53.

Kunci Kondisi Rute 53	Operasi API	Tipe nilai	Deskripsi
<code>route53:ChangeResourceRecordSetsNormalizedRecordNames</code>	ChangeResourceRecordSets	Multi-nilai	Merupakan daftar nama catatan DNS dalam permintaan. <code>ChangeResourceRecordSets</code> Untuk mendapatkan perilaku yang diharapkan, nama DNS dalam kebijakan IAM harus dinormalisasi sebagai berikut: • Semua huruf harus huruf kecil. • Nama DNS harus tanpa trailing dot. • Karakter selain a hingga z, 0 hingga 9, - (tanda hubung), _ (garis bawah), dan. (periode, sebagai pembatas antara label) harus menggunakan kode escape dalam format \ kode oktal tiga digit.
<code>route53:ChangeResourceRecordSetTypes</code>	ChangeResourceRecordSets	Multi-nilai	Merupakan daftar jenis catatan DNS dalam permintaan. <code>ChangeResourceRecordSets</code> <code>ChangeResourceRecordSetTypes</code> dapat berupa salah satu jenis catatan DNS yang didukung Route 53. Untuk informasi selengkapnya, lihat Tipe data DNS yang didukung. Semua harus dimasukkan dalam huruf besar dalam kebijakan.
<code>route53:ChangeResourceRecordSetActions</code>	ChangeResourceRecordSets	Multi-nilai	Merupakan daftar tindakan dalam permintaan <code>ChangeResourceRecordSets</code>. <code>ChangeResourceRecordSetActions</code> dapat berupa salah satu dari nilai berikut (harus huruf besar): • CREATE

Kunci Kondisi Rute 53	Operasi API	Tipe nilai	Deskripsi
			• MENEGAKKAN • DELETE
route53:VPCs	Rekanan VPCWith HostedZone Putus hubungan VPCFrom HostedZone ListHostedZonesByVPC CreateHostedZone Buat VPCAssociation Otorisasi Hapus VPCAssociation Otorisasi	Multi-nilai	Merupakan daftar VPCs dalam permintaanAssociateVPCWithHostedZone, DisassociateVPCFromHostedZone, ListHostedZonesByVPC, CreateHostedZone, CreateVPCAssociationAuthorization, danDeleteVPCAssociationAuthorization, dalam format "VPCId=<vpc-id>, VPCRegion = <region>

Contoh kebijakan: Menggunakan kondisi untuk akses berbutir halus

Setiap contoh di bagian ini menetapkan klausa Efek ke Izinkan dan hanya menentukan tindakan, sumber daya, dan parameter yang diizinkan. Akses hanya diizinkan untuk apa yang tercantum secara eksplisit dalam kebijakan IAM.

Dalam beberapa kasus, dimungkinkan untuk menulis ulang kebijakan ini sehingga berbasis penolakan (yaitu, menyetel klausa Efek ke Deny dan membalikkan semua logika dalam kebijakan). Namun, kami menyarankan Anda menghindari penggunaan kebijakan berbasis penolakan karena sulit ditulis dengan benar, dibandingkan dengan kebijakan berbasis izin. Hal ini terutama berlaku untuk Route 53 karena normalisasi teks yang diperlukan.

Berikan izin yang membatasi akses ke catatan DNS dengan nama tertentu

Kebijakan izin berikut memberikan izin yang mengizinkan `ChangeResourceRecordSets` tindakan di Zona Hosted Z12345 untuk `example.com` dan `marketing.example.com`. Ini menggunakan tombol `route53:ChangeResourceRecordSetsNormalizedRecordNames` kondisi untuk membatasi tindakan pengguna hanya pada catatan yang cocok dengan nama yang ditentukan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z111111122222233333",
      "Condition": {
        "ForAllValues:StringEquals": {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames":
            ["example.com", "marketing.example.com"]
        }
      }
    }
  ]
}
```

`ForAllValues:StringEquals` adalah operator kondisi IAM yang berlaku untuk kunci multi-nilai. Kondisi dalam kebijakan di atas akan memungkinkan operasi hanya ketika semua perubahan

ChangeResourceRecordSets memiliki nama DNS example.com. Untuk informasi selengkapnya, lihat [operator kondisi IAM](#) dan [kondisi IAM dengan beberapa kunci atau nilai](#) dalam Panduan Pengguna IAM.

Untuk menerapkan izin yang cocok dengan nama dengan sufiks tertentu, Anda dapat menggunakan wildcard IAM (*) dalam kebijakan dengan operator kondisi atau. StringLike StringNotLike Kebijakan berikut akan memungkinkan operasi ketika semua perubahan dalam ChangeResourceRecordSets operasi memiliki nama DNS yang diakhiri dengan “-beta.example.com”.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z1111111222222333333",
      "Condition": {
        "ForAllValues:StringLike": {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames":
            ["*-beta.example.com"]
        }
      }
    }
  ]
}
```

Note

Wildcard IAM tidak sama dengan wildcard nama domain. Lihat contoh berikut untuk cara menggunakan wildcard dengan nama domain.

Berikan izin yang membatasi akses ke catatan DNS yang cocok dengan nama domain yang berisi wildcard

Kebijakan izin berikut memberikan izin yang mengizinkan `ChangeResourceRecordSets` tindakan di Zona Dihosting Z12345 untuk `example.com`. Ini menggunakan kunci `route53:ChangeResourceRecordSetsNormalizedRecordNames` kondisi untuk membatasi tindakan pengguna hanya untuk catatan yang cocok `*.example.com`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z11111112222222333333",
      "Condition": {
        "ForAllValues:StringEquals": {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames": [
            "\052.example.com"
          ]
        }
      }
    }
  ]
}
```

`\052` adalah kode oktal untuk karakter `*` dalam nama DNS, dan `\` in diloloskan `\\` untuk mengikuti `\052` sintaks JSON.

Berikan izin yang membatasi akses ke catatan DNS tertentu

Kebijakan izin berikut memberikan izin yang mengizinkan `ChangeResourceRecordSets` tindakan di Zona Dihosting Z12345 untuk `example.com`. Ini menggunakan kombinasi tiga tombol kondisi untuk membatasi tindakan pengguna untuk memungkinkan hanya membuat atau mengedit catatan DNS dengan nama dan jenis DNS tertentu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z1111111222222333333",
      "Condition": {
        "ForAllValues:StringEquals":{
          "route53:ChangeResourceRecordSetsNormalizedRecordNames":
["example.com"],
          "route53:ChangeResourceRecordSetsRecordTypes": ["MX"],
          "route53:ChangeResourceRecordSetsActions": ["CREATE",
"UPSERT"]
        }
      }
    }
  ]
}

```

Berikan izin yang membatasi akses untuk membuat dan mengedit hanya jenis catatan DNS yang ditentukan

Kebijakan izin berikut memberikan izin yang mengizinkan ChangeResourceRecordSets tindakan di Zona Dihosting Z12345 untuk example.com. Ini menggunakan tombol route53:ChangeResourceRecordSetsRecordTypes kondisi untuk membatasi tindakan pengguna hanya pada catatan yang cocok dengan jenis yang ditentukan (A dan AAAA).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "route53:ChangeResourceRecordSets",
      "Resource": "arn:aws:route53::hostedzone/Z1111111222222333333",
      "Condition": {
        "ForAllValues:StringEquals":{
          "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
        }
      }
    }
  ]
}

```

```
}
```

Berikan izin yang menentukan VPC tempat prinsipal IAM dapat beroperasi

Kebijakan izin berikut memberikan izin yang mengizinkan `AssociateVPCWithHostedZone`, `DisassociateVPCFromHostedZone`, `ListHostedZonesByVPC`, `CreateHostedZone`, `CreateVPCAssociationAuthorization`, dan `DeleteVPCAssociationAuthorization` tindakan pada VPC yang ditentukan oleh `vpc-id`.

Important

Nilai kondisi harus dalam format `VPCId=<vpc-id>,VPCRegion=<region>`. Jika Anda menentukan VPC ARN dalam nilai kondisi, kunci kondisi tidak akan berlaku.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "route53:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "route53:VPCs": [
            "VPCId=<vpc-id>,VPCRegion=<region>"
          ]
        }
      }
    },
    {
      "Sid": "Statement2",
      "Effect": "Allow",
```

```
        "Action": "ec2:DescribeVpcs",
        "Resource": "*"
    }
}
```

Izin API Amazon Route 53: Referensi tindakan, sumber daya, dan syarat

Saat menyiapkan [Kontrol akses](#) dan menulis kebijakan izin yang dapat dilampirkan ke identitas IAM (kebijakan berbasis identitas), Anda dapat menggunakan daftar Tindakan, sumber daya, dan kunci kondisi [untuk kunci Route 53, Tindakan, sumber daya, dan kondisi untuk Route 53 Domain, Tindakan, sumber daya, dan kunci kondisi untuk Resolver VPC, serta kunci Tindakan, sumber daya, dan kondisi untuk Profil Amazon Route 53 memungkinkan berbagi pengaturan DNS](#) dengan in Referensi Otorisasi Layanan. VPCs Halaman tersebut menyertakan setiap tindakan Amazon Route 53 API, tindakan yang harus Anda berikan akses izin, dan AWS sumber daya yang harus Anda berikan akses. Anda menentukan tindakan dalam bidang `Action` kebijakan, dan Anda menentukan nilai sumber daya pada bidang `Resource` kebijakan.

Anda dapat menggunakan tombol kondisi AWS-wide dalam kebijakan Route 53 Anda untuk menyatakan kondisi. Untuk daftar lengkap tombol AWS-wide, lihat Kunci yang [tersedia](#) di Panduan Pengguna IAM.

Note

Saat memberikan akses, zona yang dihosting dan VPC Amazon harus milik partisi yang sama. Partisi adalah sekelompok Wilayah AWS. Masing-masing Akun AWS dicakup ke satu partisi.

Berikut ini adalah partisi yang didukung:

- `aws` - Wilayah AWS
- `aws-cn` - Wilayah Tiongkok
- `aws-us-gov` - AWS GovCloud (US) Region

Untuk informasi selengkapnya, lihat [Manajemen Akses](#) di Referensi AWS Umum.

 Note

Untuk menentukan tindakan, gunakan awalan (`route53`, `route53domains`, atau `route53resolver`) diikuti dengan nama operasi API, misalnya:

- `route53:CreateHostedZone`
- `route53domains:RegisterDomain`
- `route53resolver:CreateResolverEndpoint`

Mencatat log dan memantau di Amazon Route 53

Amazon Route 53 menyediakan pencatatan kueri DNS dan kemampuan untuk memantau sumber daya Anda menggunakan pemeriksaan kondisi. Selain itu, Route 53 terintegrasi dengan AWS layanan lain untuk menyediakan pencatatan dan pemantauan tambahan:

Memantau kueri DNS

Anda dapat mengonfigurasi Route 53 untuk mencatat informasi tentang permintaan yang menerima Route 53, seperti domain atau subdomain yang diminta, tanggal dan waktu permintaan, dan jenis data DNS, seperti A atau AAAA.

Untuk informasi selengkapnya, lihat [Pencatatan kueri DNS publik](#).

Menggunakan AWS CloudTrail untuk mencatat konsol dan tindakan terprogram

CloudTrail menyediakan catatan tindakan Route 53 yang diambil oleh pengguna, peran, atau AWS layanan. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat melacak permintaan yang dibuat, alamat IP tempat permintaan berasal, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat [Mencatat panggilan API Amazon Route 53 dengan AWS CloudTrail](#).

Memantau pendaftaran domain

Dasbor Route 53 menyediakan informasi mendetail tentang status pendaftaran domain Anda, seperti status transfer domain dan domain yang mendekati tanggal kedaluwarsa.

Untuk informasi selengkapnya, lihat [Memantau pendaftaran domain](#).

Menggunakan pemeriksaan kesehatan Route 53 dan Amazon CloudWatch untuk memantau sumber daya Anda

Anda dapat memantau sumber daya Anda dengan membuat pemeriksaan kesehatan Route 53, yang digunakan CloudWatch untuk mengumpulkan dan memproses data mentah menjadi metrik yang dapat dibaca, mendekati waktu nyata.

Untuk informasi selengkapnya, lihat [Memantau sumber daya Anda dengan pemeriksaan kesehatan Amazon Route 53 dan Amazon CloudWatch](#).

Menggunakan Amazon CloudWatch untuk memantau titik akhir Route 53 VPC Resolver

Anda dapat menggunakan CloudWatch untuk memantau jumlah kueri DNS yang diteruskan oleh titik akhir Resolver.

Untuk informasi selengkapnya, lihat [Memantau Route 53 titik akhir VPC Resolver dengan Amazon CloudWatch](#).

Menggunakan AWS Trusted Advisor

Trusted Advisor mengacu pada praktik terbaik yang dipelajari dari melayani AWS pelanggan. Trusted Advisor memeriksa AWS lingkungan Anda dan kemudian membuat rekomendasi ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan. Semua AWS pelanggan memiliki akses ke lima Trusted Advisor cek. Pelanggan dengan paket dukungan Bisnis atau Perusahaan dapat melihat semua Trusted Advisor pemeriksaan.

Untuk informasi selengkapnya, lihat [Trusted Advisor](#).

Validasi kepatuhan untuk Amazon Route 53

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon Route 53 sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#). Untuk informasi umum, lihat [Program Kepatuhan AWS](#).

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh laporan di AWS Artifak](#).

Tanggung jawab kepatuhan Anda saat menggunakan Route 53 ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. Jika penggunaan Route 53 Anda tunduk pada kepatuhan terhadap standar seperti HIPAA, PCI, atau FedRAMP, menyediakan sumber daya untuk membantu: AWS

- [Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- [Merancang Laporan Resmi Keamanan dan Kepatuhan HIPAA](#) – Laporan resmi ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.
- [AWS Sumber Daya Kepatuhan](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Config](#) AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub CSPM](#)— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Amazon Route 53

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Route 53 membagi fungsinya menjadi kontrol dan bidang data. Layanan Route 53, seperti kebanyakan AWS layanan, mencakup bidang kontrol yang memungkinkan Anda melakukan operasi manajemen seperti membuat, memperbarui, dan menghapus sumber daya, dan bidang data yang menyediakan fungsionalitas inti layanan. Untuk informasi selengkapnya tentang bidang kontrol dan data di Route 53, lihat [Konsep bidang kontrol dan data](#).

Route 53 terutama merupakan layanan global, tetapi fitur berikut mendukung AWS Wilayah:

- Jika Anda menggunakan Route 53 VPC Resolver untuk menyiapkan konfigurasi hibrida, Anda membuat titik akhir di AWS Wilayah yang Anda pilih, dan Anda menentukan alamat IP di beberapa Availability Zone. Untuk titik akhir keluar, Anda membuat aturan di Wilayah yang sama di mana Anda membuat titik akhir. Untuk informasi selengkapnya, lihat [Apa itu Route 53 VPC Resolver?](#).
- Anda dapat mengonfigurasi pemeriksaan kondisi Route 53 untuk memeriksa kondisi sumber daya yang Anda buat di wilayah tertentu, seperti instans Amazon EC2 dan penyeimbang beban Elastic Load Balancing.
- Saat Anda membuat pemeriksaan kesehatan yang memantau titik akhir, Anda dapat secara opsional menentukan Wilayah yang Anda inginkan dari Route 53 untuk melakukan pemeriksaan kondisi.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Keamanan Infrastruktur di Amazon Route 53

Sebagai layanan terkelola, Amazon Route 53 dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Route 53 melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Mengirim temuan dari Resolver DNS Firewall ke Security Hub CSPM

[AWS Security Hub CSPM](#) memberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub CSPM mengumpulkan data keamanan dari seluruh Akun AWS Layanan AWS, dan mendukung produk mitra pihak ketiga, serta membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

Dengan mengintegrasikan Resolver DNS Firewall dengan Security Hub CSPM, Anda dapat mengirim temuan dari DNS Firewall ke Security Hub CSPM. Security Hub CSPM kemudian memasukkan temuan-temuan tersebut dalam analisisnya tentang postur keamanan Anda.

Daftar Isi

- [Cara kerja temuan di Security Hub CSPM](#)
 - [Jenis temuan yang dikirim DNS Firewall](#)
 - [Mencoba lagi saat CSPM Security Hub tidak tersedia](#)
 - [Memperbarui temuan yang ada di Security Hub CSPM](#)
- [Temuan khas dari DNS Firewall](#)
- [Mengaktifkan dan mengonfigurasi integrasi](#)
- [Menghentikan pengiriman temuan ke Security Hub CSPM](#)

Cara kerja temuan di Security Hub CSPM

Dalam Security Hub CSPM, temuan adalah catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Beberapa temuan berasal dari masalah yang terdeteksi oleh pihak lain Layanan AWS atau oleh mitra pihak ketiga. Security Hub CSPM juga memiliki kontrol keamanan sendiri yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub CSPM menyediakan alat untuk mengelola temuan dari seluruh sumber ini. Anda dapat melihat dan memfilter daftar temuan dan melihat detail temuan. Untuk selengkapnya, lihat [Meninjau detail pencarian dan menemukan riwayat di CSPM Security Hub di Panduan Pengguna.AWS Security Hub](#) Anda juga dapat memperbarui temuan secara otomatis atau mengirimkannya ke tindakan khusus. Untuk informasi selengkapnya, lihat [Secara otomatis memodifikasi dan mengambil tindakan pada temuan CSPM Security Hub](#) di Panduan Pengguna.AWS Security Hub

Semua temuan di Security Hub CSPM menggunakan format JSON standar yang disebut AWS Security Finding Format (ASFF). ASFF mencakup rincian tentang sumber masalah keamanan, sumber daya yang terpengaruh, dan status temuan saat ini. Untuk informasi selengkapnya, lihat [AWS Security Finding Format \(ASFF\)](#) di Panduan Pengguna AWS Security Hub .

DNS Firewall adalah salah satu Layanan AWS yang mengirimkan temuan ke Security Hub CSPM.

Jenis temuan yang dikirim DNS Firewall

DNS Firewall memiliki integrasi berikut:

- Daftar Domain Terkelola: temuan keamanan yang terkait dengan kueri yang diblokir atau diperingatkan untuk domain yang terkait dengan Daftar Domain AWS Terkelola.
- Daftar domain khusus: temuan keamanan yang terkait dengan kueri yang diblokir atau diperingatkan untuk domain yang terkait dengan daftar domain pelanggan.
- DNS Firewall Advanced: temuan keamanan yang terkait dengan kueri yang diblokir atau diperingatkan oleh DNS Firewall Advanced.

Security Hub CSPM menyerap temuan dari DNS Firewall dalam [AWS Security Finding Format](#) (ASFF). Dalam ASFF, bidang Types menyediakan jenis temuan. Temuan dari DNS Firewall dapat memiliki nilai berikut untuk Types.

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Mencoba lagi saat CSPM Security Hub tidak tersedia

Jika Security Hub CSPM tidak tersedia, DNS Firewall mencoba mengirim ulang temuan sampai mereka diterima.

Memperbarui temuan yang ada di Security Hub CSPM

DNS Firewall akan memperbarui temuan yang ada jika temuan yang sama diamati lagi.

Temuan khas dari DNS Firewall

Security Hub CSPM menyerap temuan DNS Firewall dalam [AWS Security Finding Format](#) (ASFF).

Berikut adalah contoh temuan khas dari DNS Firewall di ASFF.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "00000000-0000-0000-0000-example1",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-resolver-dns-firewall-aws-list",
  "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-rule-group/rslvr-frg-example1",
  "AwsAccountId": "000000000000",
  "Types": [
    "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
  ],
  "FirstObservedAt": "2024-12-06T19:58:49.000Z",
  "LastObservedAt": "2024-12-06T19:58:49.000Z",
  "CreatedAt": "2024-12-06T19:58:49.000Z",
  "UpdatedAt": "2024-12-06T19:58:49.000Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC vpc-example1",
  "Description": "DNS Firewall ALERT",
  "ProductFields": {
    "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
    "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-example1",
    "aws/route53resolver/dnsfirewall/queryType": "A",
    "aws/route53resolver/dnsfirewall/queryClass": "IN",
    "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-example1",
    "aws/route53resolver/dnsfirewall/transport": "UDP",
    "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/amazon/route-53-resolver-dns-firewall-aws-list/00000000-0000-0000-0000-example1",
    "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS List",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
```

```

    {
      "Type": "Other",
      "Id": "rslvr-in-example1",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "Other": {
          "ResourceType": "ResolverEndpoint",
          "EndpointId": "rslvr-in-example1"
        }
      }
    },
    {
      "Type": "Other",
      "Id": "rni-example1",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "Other": {
          "NetworkInterfaceId": "rni-example1",
          "ResourceType": "ResolverNetworkInterface"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
    ]
  },
  "ProcessedAt": "2024-12-11T19:33:35.494Z"
}

```


Mengaktifkan dan mengonfigurasi integrasi

Untuk mengintegrasikan DNS Firewall dengan Security Hub CSPM, Anda harus terlebih dahulu mengaktifkan Security Hub CSPM. Untuk informasi tentang mengaktifkan CSPM Security Hub, lihat Mengaktifkan CSPM [Security Hub](#) di Panduan Pengguna.AWS Security Hub

Menghentikan pengiriman temuan ke Security Hub CSPM

Untuk menghentikan pengiriman temuan DNS Firewall ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Untuk petunjuk, lihat [Menonaktifkan alur temuan dari integrasi](#) dalam AWS Security Hub Panduan Pengguna.

Memantau Amazon Route 53

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. Namun sebelum mulai memantau; Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan berikut:

- Apa sasaran pemantauan Anda?
- Sumber daya apa yang akan Anda pantau?
- Seberapa sering Anda akan memantau sumber daya ini?
- Alat pemantauan apa yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Topik

- [Pencatatan kueri DNS publik](#)
- [Pencatatan kueri penyelesai](#)
- [Memantau pendaftaran domain](#)
- [Memantau sumber daya Anda dengan pemeriksaan kesehatan Amazon Route 53 dan Amazon CloudWatch](#)
- [Memantau zona yang dihosting menggunakan Amazon CloudWatch](#)
- [Memantau Route 53 titik akhir VPC Resolver dengan Amazon CloudWatch](#)
- [Memantau grup aturan DNS Firewall Resolver dengan Amazon CloudWatch](#)
- [Mengelola peristiwa Resolver DNS Firewall menggunakan Amazon EventBridge](#)
- [Mencatat panggilan API Amazon Route 53 dengan AWS CloudTrail](#)

Pencatatan kueri DNS publik

Anda dapat mengonfigurasi Amazon Route 53 untuk mencatat informasi tentang kueri DNS publik yang diterima Route 53, seperti berikut:

- Domain atau subdomain yang diminta

- Tanggal dan waktu permintaan
- Tipe catatan DNS (seperti A atau AAAA)
- Lokasi edge Route 53 yang merespons kueri DNS
- Kode respons DNS, seperti `NoError` atau `ServFail`

Setelah Anda mengonfigurasi pencatatan kueri, Route 53 akan mengirim CloudWatch log ke Log. Anda menggunakan alat CloudWatch Log untuk mengakses log kueri.

Log kueri hanya berisi kueri yang dikirim oleh penyelesai DNS ke Route 53. Jika resolver DNS telah men-cache respons ke kueri (seperti alamat IP untuk penyeimbang beban untuk `example.com`), resolver akan terus mengembalikan respons yang di-cache tanpa mengirim kueri ke Route 53 hingga TTL untuk catatan yang sesuai kedaluwarsa.

Tergantung pada jumlah kueri DNS yang dikirim untuk nama domain (`example.com`) atau nama subdomain (`www.example.com`), penyelesai yang digunakan pengguna, dan TTL untuk catatan, log kueri mungkin berisi informasi tentang satu kueri saja dari beberapa ribu kueri yang dikirimkan ke penyelesai DNS. Untuk informasi selengkapnya tentang cara kerja DNS, lihat [Cara lalu lintas internet dirutekan ke situs web atau aplikasi web Anda](#).

Jika Anda tidak memerlukan informasi pencatatan terperinci, Anda dapat menggunakan CloudWatch metrik Amazon untuk melihat jumlah total kueri DNS yang ditanggapi Route 53 untuk zona yang dihosting. Untuk informasi selengkapnya, lihat [Melihat metrik kueri DNS untuk zona yang di-hosting publik](#).

Topik

- [Mengonfigurasi pencatatan untuk kueri DNS](#)
- [Menggunakan Amazon CloudWatch untuk mengakses log kueri DNS](#)
- [Mengubah periode retensi untuk log dan mengeksport log ke Amazon S3](#)
- [Menghentikan pencatatan kueri](#)
- [Nilai-nilai yang muncul di log kueri DNS](#)
- [Contoh log kueri](#)

Mengonfigurasi pencatatan untuk kueri DNS

Untuk mulai mencatat kueri DNS untuk zona yang di-hosting tertentu, lakukan tugas berikut di konsol Amazon Route 53:

- Pilih grup CloudWatch log yang Anda inginkan Route 53 untuk memublikasikan log, atau buat grup log baru.

 Note

Grup log harus berada di Wilayah US East (N. Virginia).

- Pilih Create (Buat) untuk menyelesaikan.

 Note

Jika pengguna mengirimkan kueri DNS untuk domain Anda, Anda harus mulai melihat kueri di log dalam beberapa menit setelah Anda membuat konfigurasi pencatatan kueri.

Cara mengonfigurasi pencatatan untuk kueri DNS

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih zona yang di-hosting dengan pencatatan kueri yang ingin Anda konfigurasi.
4. Di panel Detail zona yang di-hosting, pilih Konfigurasi pencatatan kueri.
5. Pilih grup log yang sudah ada atau buat grup log baru.
6. Jika Anda menerima peringatan tentang izin (ini terjadi jika Anda belum mengonfigurasi pencatatan kueri dengan konsol baru), lakukan salah satu tindakan berikut:
 - Jika sudah memiliki 10 kebijakan sumber daya, Anda tidak dapat membuatnya lagi. Pilih salah satu kebijakan sumber daya, dan pilih Edit. Pengeditan akan memberikan izin kepada Route 53 untuk menulis log ke grup log Anda. Pilih Simpan. Peringatan akan hilang dan Anda dapat melanjutkan ke langkah berikutnya.
 - Jika Anda belum pernah mengonfigurasi pencatatan kueri sebelumnya (atau jika Anda belum membuat 10 kebijakan sumber daya), Anda perlu memberikan izin ke Route 53 untuk menulis log ke grup CloudWatch Log Anda. Pilih Berikan izin. Peringatan akan hilang dan Anda dapat melanjutkan ke langkah berikutnya.

7. Pilih Izin - opsional untuk melihat tabel yang menunjukkan apakah kebijakan sumber daya cocok dengan grup CloudWatch log, dan apakah Route 53 memiliki izin untuk memublikasikan log. CloudWatch
8. Pilih Buat.

Menggunakan Amazon CloudWatch untuk mengakses log kueri DNS

Amazon Route 53 mengirimkan log kueri langsung ke CloudWatch Log; log tidak pernah dapat diakses melalui Route 53. Sebagai gantinya, Anda menggunakan CloudWatch Log untuk melihat log dalam waktu dekat, mencari dan memfilter data, dan mengekspor log ke Amazon S3.

Route 53 membuat satu aliran CloudWatch log Log untuk setiap lokasi tepi Route 53 yang merespons kueri DNS untuk zona host yang ditentukan dan mengirimkan log kueri ke aliran log yang berlaku. Format untuk nama setiap aliran log adalah *hosted-zone-id/edge-location-ID*, misalnya, `Z1D633PJN98FT9/DFW3`.

Setiap lokasi tepi diidentifikasi oleh kode tiga huruf dan nomor yang ditetapkan secara sewenang-wenang, misalnya, DFW3. Kode tiga huruf biasanya sesuai dengan kode bandara International Air Transport Association untuk bandara yang berada di dekat lokasi tepi. (Ringkasan ini mungkin berubah di masa mendatang.) Untuk daftar lokasi edge, lihat "The Route 53 Global Network" pada halaman [Detail Produk Route 53](#).

Note

Anda mungkin melihat beberapa awalan atau sufiks yang tidak mengikuti konvensi di atas. Mereka menyandikan atribut yang hanya untuk penggunaan internal.

Untuk informasi lebih lanjut, lihat dokumentasi yang berlaku:

- [Panduan Pengguna Amazon CloudWatch Logs](#)
- [Referensi API Amazon CloudWatch Logs](#)
- [CloudWatch Bagian log dari Referensi AWS CLI Perintah](#)
- [Nilai-nilai yang muncul di log kueri DNS](#)

Mengubah periode retensi untuk log dan mengekspor log ke Amazon S3

Secara default, CloudWatch Log menyimpan log kueri tanpa batas waktu. Anda dapat menentukan periode retensi secara opsional sehingga CloudWatch Log menghapus log yang lebih lama dari periode penyimpanan. Untuk informasi selengkapnya, lihat [Mengubah penyimpanan data CloudWatch log di Log](#) di Panduan CloudWatch Pengguna Amazon.

Jika Anda ingin menyimpan data log tetapi Anda tidak memerlukan alat CloudWatch Log untuk melihat dan menganalisis data, Anda dapat mengekspor log ke Amazon S3, yang dapat mengurangi biaya penyimpanan Anda. Untuk informasi lebih lanjut, lihat [Mengekspor data log ke Amazon S3](#).

Untuk informasi tentang harga, lihat halaman harga yang berlaku:

- “CloudWatch Log Amazon” di halaman [CloudWatch Harga](#)
- [Harga Amazon S3](#)

Note

Saat mengonfigurasi Route 53 untuk mencatat kueri DNS, Anda tidak dikenakan biaya Route 53.

Menghentikan pencatatan kueri

Jika Anda ingin Amazon Route 53 berhenti mengirim log kueri ke CloudWatch Log, lakukan prosedur berikut untuk menghapus konfigurasi pencatatan kueri.

Cara menghapus konfigurasi pencatatan kueri

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih nama untuk zona yang di-hosting dengan konfigurasi pencatatan kueri yang ingin Anda hapus.
4. Di panel Detail zona yang di-hosting, pilih Hapus konfigurasi pencatatan kueri.
5. Pilih Hapus untuk mengonfirmasi.

Nilai-nilai yang muncul di log kueri DNS

Setiap file log berisi satu entri log untuk setiap kueri DNS yang diterima Amazon Route 53 dari penyelesaian DNS di lokasi edge yang sesuai. Setiap entri log mencakup nilai-nilai berikut:

Versi format log

Nomor versi log kueri ini. Jika kita menambahkan bidang ke log atau mengubah format bidang yang ada, kita akan menambahkan nilai ini.

Timestamp kueri

Tanggal dan waktu Route 53 merespons permintaan, dalam format ISO 8601 dan Coordinated Universal Time (UTC), misalnya, 2017-03-16T19:20:25.177Z.

Untuk informasi tentang format ISO 8601, lihat artikel Wikipedia [ISO 8601](#). Untuk informasi tentang UTC, lihat artikel Wikipedia [Coordinated Universal Time](#).

ID zona yang di-hosting

ID zona yang di-hosting yang terkait dengan semua kueri DNS dalam log ini.

Nama kueri

Domain atau subdomain yang ditentukan dalam permintaan.

Jenis kueri

Jenis catatan DNS yang ditentukan dalam permintaan, atau ANY. Untuk informasi tentang jenis yang didukung Route 53, lihat [Tipe data DNS yang didukung](#).

Kode respons

Kode respons DNS yang Route 53 dikembalikan dalam menanggapi kueri DNS.

Protokol Layer 4

Protokol yang digunakan untuk mengirimkan kueri, baik TCP atau UDP.

Lokasi edge Route 53

Lokasi edge Route 53 yang merespons kueri. Setiap lokasi tepi diidentifikasi oleh kode tiga huruf dan nomor arbitrer, misalnya, DFW3. Kode tiga huruf biasanya sesuai dengan kode bandara International Air Transport Association untuk bandara yang berada di dekat lokasi tepi. (Ringkasan ini mungkin berubah di masa mendatang.)

Untuk daftar lokasi edge, lihat "The Route 53 Global Network" pada halaman [Detail Produk Route 53](#).

Alamat IP penyelesai

Alamat IP penyelesai DNS yang mengirimkan permintaan ke Route 53.

Subnet klien EDNS

Alamat IP parsial untuk klien tempat permintaan berasal, jika tersedia dari penyelesai DNS.

Untuk informasi lebih lanjut, lihat draf IETF [Subnet Klien dalam Permintaan DNS](#).

Contoh log kueri

Berikut contoh log kueri (Region adalah placeholder):

```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP Region 192.168.1.1
-
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP Region
192.168.3.1 192.168.222.0/24
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP Region
2001:db8::1234 2001:db8:abcd::/48
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP Region
192.168.3.1 192.168.111.0/24
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP Region
192.168.1.2 -
```

Pencatatan kueri penyelesai

Anda dapat mencatat kueri DNS berikut:

- Kueri yang berasal dari Amazon Virtual Private Cloud VPCs yang Anda tentukan, serta tanggapan terhadap kueri DNS tersebut.
- Kueri dari sumber daya on-premise yang menggunakan titik akhir Resolver masuk.
- Kueri yang menggunakan titik akhir Resolver keluar untuk resolusi DNS rekursif.
- Kueri yang menggunakan aturan Resolver DNS Firewall untuk memblokir, mengizinkan, atau memantau daftar domain.

Log kueri VPC Resolver menyertakan nilai-nilai seperti berikut ini:

- AWS Wilayah tempat VPC dibuat
- ID VPC tempat kueri berasal
- Alamat IP instans tempat kueri berasal
- ID instans sumber daya tempat kueri berasal
- Tanggal dan waktu pertama kali kueri dibuat
- Nama DNS yang diminta (seperti prod.example.com)
- Jenis catatan DNS (seperti A atau AAAA)
- Kode respons DNS, seperti `NoError` atau `ServFail`
- Data respons DNS, seperti alamat IP yang dikembalikan dalam merespons kueri DNS
- Respons terhadap tindakan aturan Firewall DNS

Untuk daftar detail dari semua nilai yang dicatat dan contoh, lihat [Nilai yang muncul di log kueri VPC Resolver](#).

Note

Seperti standar untuk resolver DNS, resolver cache DNS query untuk jangka waktu yang ditentukan oleh (TTL) untuk resolver. time-to-live Resolver VPC Route 53 menyimpan kueri yang berasal dari Anda VPCs, dan merespons dari cache bila memungkinkan untuk mempercepat respons. Pencatatan kueri VPC Resolver hanya mencatat kueri unik, bukan kueri yang dapat ditanggapi oleh VPC Resolver dari cache.

Misalnya, misalkan instans EC2 di salah satu konfigurasi pencatatan kueri untuk mencatat kueri, mengirimkan permintaan untuk `accounting.example.com`. VPCs VPC Resolver menyimpan respons terhadap kueri itu, dan mencatat kueri. Jika elastic network interface instance yang sama membuat kueri untuk `accounting.example.com` dalam TTL cache VPC Resolver, VPC Resolver merespons kueri dari cache. Kueri kedua tidak dicatat.

Anda dapat mengirim log ke salah satu AWS sumber daya berikut:

- Grup CloudWatch log Amazon CloudWatch Log (Log)
- Bucket Amazon S3 (S3)
- Aliran pengiriman Firehose

Untuk informasi selengkapnya, lihat [AWS sumber daya yang dapat Anda kirim log kueri VPC Resolver](#).

Topik

- [AWS sumber daya yang dapat Anda kirim log kueri VPC Resolver](#)
- [Mengelola konfigurasi pencatatan kueri Resolver](#)

AWS sumber daya yang dapat Anda kirim log kueri VPC Resolver

Note

Jika ingin mencatat kueri untuk beban kerja dengan kueri tinggi per detik (QPS), Anda harus menggunakan Amazon S3 untuk memastikan log kueri Anda tidak di-throttle ketika ditulis ke tujuan Anda. Jika Anda menggunakan Amazon CloudWatch, Anda dapat meningkatkan batas permintaan per detik untuk PutLogEvents operasi. Untuk mempelajari lebih lanjut tentang meningkatkan CloudWatch batas, lihat [Kuota CloudWatch log](#) di Panduan CloudWatch Pengguna Amazon.

Anda dapat mengirim log kueri VPC Resolver ke sumber daya berikut: AWS

Grup CloudWatch log Amazon CloudWatch Logs (Amazon Logs)

Anda dapat menganalisis log dengan Wawasan Log serta membuat metrik dan alarm.

Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon CloudWatch Logs](#).

Bucket Amazon S3 (S3)

Bucket S3 memiliki harga yang ekonomis untuk pengarsipan log jangka panjang. Latensi biasanya lebih tinggi.

Semua opsi enkripsi sisi server S3 didukung. Untuk informasi selengkapnya, lihat [Melindungi data dengan enkripsi sisi server di Panduan](#) Pengguna Amazon S3.

Jika Anda memilih Enkripsi Sisi Server dengan AWS KMS Kunci (SSE-KMS), Anda harus memperbarui kebijakan kunci untuk kunci yang dikelola pelanggan agar akun pengiriman log dapat menulis ke bucket Amazon S3 Anda. Untuk informasi selengkapnya tentang kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS, lihat enkripsi [sisi server bucket Amazon S3 di Panduan Pengguna](#) Amazon. CloudWatch

Jika bucket S3 ada di akun yang Anda miliki, izin yang diperlukan akan ditambahkan secara otomatis ke kebijakan bucket Anda. Jika ingin mengirim log ke bucket S3 di akun yang tidak Anda miliki, pemilik bucket S3 harus menambahkan izin untuk akun Anda dalam kebijakan bucket mereka. Contoh:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "CrossAccountAccess",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::your_bucket_name/
AWSLogs/your_caller_account/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::your_bucket_name"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "iam_user_arn_or_account_number_for_root"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::your_bucket_name"
    }
  ]
}
```

Note

Jika ingin menyimpan log di bucket S3 sentral untuk organisasi Anda, kami sarankan Anda menyiapkan konfigurasi pencatatan kueri dari akun terpusat (dengan izin yang diperlukan untuk menulis ke bucket sentral) dan menggunakan [RAM](#) untuk berbagi konfigurasi di seluruh akun.

Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon Simple Storage Service](#).

Aliran pengiriman Firehose

Anda dapat melakukan streaming log secara real time ke Amazon OpenSearch Service, Amazon Redshift, atau aplikasi lain.

Untuk informasi selengkapnya, lihat Panduan [Pengembang Amazon Data Firehose](#).

Untuk informasi tentang harga untuk pencatatan kueri Resolver, lihat harga [Amazon CloudWatch](#).

CloudWatch Biaya Vending Logs berlaku saat menggunakan log Resolver VPC, bahkan ketika log dipublikasikan langsung ke Amazon S3. Untuk informasi selengkapnya, lihat [Harga log dengan CloudWatch harga Amazon](#).

Mengelola konfigurasi pencatatan kueri Resolver

Mengkonfigurasi (pencatatan kueri VPC Resolver)

Anda dapat mengonfigurasi pencatatan kueri VPC Resolver dengan dua cara:

- Asosiasi VPC langsung - Kaitkan VPCs langsung ke konfigurasi pencatatan kueri.
- Asosiasi profil - Kaitkan konfigurasi pencatatan kueri ke Profil Route 53, yang menerapkan pencatatan ke semua yang VPCs terkait dengan Profil tersebut. Untuk informasi selengkapnya, lihat [Kaitkan konfigurasi pencatatan kueri VPC Resolver ke Profil Route 53](#).

Untuk mulai mencatat kueri DNS yang berasal dari Anda VPCs, Anda melakukan tugas berikut di konsol Amazon Route 53:

Cara mengonfigurasi pencatatan kueri Resolver

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Memperluas menu konsol Route 53. Di sudut kiri atas konsol, pilih ikon tiga bilah horizontal ().
3. Dalam menu Resolver, pilih Pencatatan kueri.
4. Di pemilih Region, pilih AWS Wilayah tempat Anda ingin membuat konfigurasi pencatatan kueri. Ini harus menjadi Wilayah yang sama tempat Anda membuat tempat Anda ingin mencatat kueri DNS. VPCs Jika Anda memiliki VPCs di beberapa Wilayah, Anda harus membuat setidaknya satu konfigurasi pencatatan kueri untuk setiap Wilayah.
5. Pilih Konfigurasi pencatatan kueri.
6. Tentukan nilai-nilai berikut ini:

Nama konfigurasi pencatatan kueri

Masukkan nama untuk konfigurasi pencatatan kueri. Nama muncul di konsol dalam daftar konfigurasi pencatatan kueri. Masukkan nama yang akan membantu Anda menemukan konfigurasi ini nanti.

Tujuan log kueri

Pilih jenis AWS sumber daya yang Anda inginkan VPC Resolver untuk mengirim log kueri. Untuk informasi tentang cara memilih di antara opsi (Grup CloudWatch log log, bucket S3, dan aliran pengiriman Firehose), lihat. [AWS sumber daya yang dapat Anda kirim log kueri VPC Resolver](#)

Setelah Anda memilih jenis sumber daya, Anda dapat membuat sumber daya lain dari jenis itu atau memilih sumber daya yang ada yang dibuat oleh AWS akun saat ini.

Note

Anda dapat memilih hanya sumber daya yang dibuat di Wilayah AWS yang Anda pilih di langkah 4, Wilayah tempat Anda membuat konfigurasi pencatatan kueri. Jika Anda memilih untuk membuat sumber daya baru, sumber daya tersebut akan dibuat di Wilayah yang sama.

VPCs untuk mencatat kueri untuk

Konfigurasi pencatatan kueri ini akan mencatat kueri DNS yang berasal dari VPCs yang Anda pilih. Centang kotak untuk setiap VPC di Wilayah saat ini yang Anda inginkan VPC Resolver untuk mencatat kueri, lalu pilih Pilih.

Alternatif: Alih-alih mengaitkan VPCs secara langsung, Anda dapat mengaitkan konfigurasi pencatatan kueri ini ke Profil Route 53, yang akan menerapkan pencatatan ke semua yang VPCs terkait dengan Profil tersebut. Untuk informasi selengkapnya, lihat [Kaitkan konfigurasi pencatatan kueri VPC Resolver ke Profil Route 53](#).

Note

Pengiriman log VPC dapat diaktifkan hanya sekali untuk jenis tujuan tertentu. Log tidak dapat dikirim ke beberapa tujuan dengan jenis yang sama, misalnya, log VPC tidak dapat dikirim ke 2 tujuan Amazon S3.

7. Pilih Konfigurasikan pencatatan kueri.

Note

Seharusnya Anda mulai melihat kueri DNS yang dibuat oleh sumber daya di VPC Anda di log dalam beberapa menit setelah berhasil membuat konfigurasi pencatatan kueri.

Nilai yang muncul di log kueri VPC Resolver

Setiap file log berisi satu entri log untuk setiap kueri DNS yang diterima Amazon Route 53 dari penyelesaian DNS di lokasi edge yang sesuai. Setiap entri log mencakup nilai-nilai berikut:

versi

Nomor versi format log kueri. Versi saat ini adalah 1.1.

Nilai versi merupakan versi utama dan minor dalam bentuk **major_version.minor_version**. Misalnya, Anda dapat memiliki nilai `version` sebesar 1.7, dengan 1 merupakan versi utama, dan 7 adalah versi minor.

Route 53 meningkatkan versi utama jika ada perubahan pada struktur log yang tidak kompatibel dengan versi sebelumnya. Ini termasuk menghapus bidang JSON yang sudah ada, atau mengubah bagaimana isi bidang direpresentasikan (misalnya, format tanggal).

Route 53 meningkatkan versi minor jika perubahan menambahkan bidang baru ke berkas log. Hal ini dapat terjadi jika informasi baru tersedia untuk beberapa atau semua kueri DNS yang ada dalam VPC.

`account_id`

ID AWS akun yang membuat VPC.

`region`

AWS Wilayah tempat Anda membuat VPC.

`vpc_id`

ID VPC tempat kueri berasal.

`query_timestamp`

Tanggal dan waktu kueri dikirimkan, dalam format ISO 8601 dan Coordinated Universal Time (UTC), misalnya, 2017-03-16T19:20:17Z.

Untuk informasi tentang format ISO 8601, lihat artikel Wikipedia [ISO 8601](#). Untuk informasi tentang UTC, lihat artikel Wikipedia [Coordinated Universal Time](#).

`query_name`

Nama domain (example.com) atau nama subdomain (www.example.com) yang ditentukan dalam kueri.

`query_type`

Jenis catatan DNS yang ditentukan dalam permintaan, atau ANY. Untuk informasi tentang jenis yang didukung Route 53, lihat [Tipe data DNS yang didukung](#).

`query_class`

Kelas kueri.

`rcode`

Kode respons DNS yang dikembalikan VPC Resolver sebagai respons terhadap kueri DNS.

Kode respons yang menunjukkan apakah kueri valid atau tidak. Kode respons yang paling umum

adalah NOERROR, yang berarti bahwa kueri tersebut valid. Jika respons tidak valid, Resolver mengembalikan kode respons yang menjelaskan alasannya. Untuk daftar kode respons yang mungkin, lihat [DNS RCODEs](#) di situs web IANA.

answer_type

Jenis catatan DNS (seperti A, MX, atau CNAME) dari nilai yang dikembalikan VPC Resolver sebagai respons terhadap kueri. Untuk informasi tentang jenis yang didukung Route 53, lihat [Tipe data DNS yang didukung](#).

rdata

Nilai yang dikembalikan VPC Resolver sebagai respons terhadap kueri. Misalnya, untuk catatan A, ini adalah alamat IP dalam IPv4 format. Untuk catatan CNAME, ini adalah nama domain dalam catatan CNAME.

answer_class

Kelas respons VPC Resolver terhadap kueri.

srcaddr

Alamat IP host yang berasal dari kueri.

srcport

Port pada instans tempat kueri berasal.

transport

Protokol yang digunakan untuk mengirimkan kueri DNS.

srcids

IDs dari `instance`, `resolver_endpoint`, dan `resolver_network_interface` bahwa kueri DNS berasal atau dilewati.

instans

ID instans tempat kueri berasal.

Note

Jika Anda melihat ID instance di log kueri Route 53 VPC Resolver yang tidak terlihat di akun Anda, itu mungkin karena kueri DNS berasal dari konsol, AWS Lambda Amazon EKS AWS CloudShell, atau Fargate, yang digunakan oleh Anda.

resolver_titik_akhir

ID titik akhir penyelesai yang melewati kueri DNS ke server DNS on-premise.

Note

Jika Anda memiliki catatan CNAME yang berantai di seluruh aturan penerusan yang berbeda menggunakan titik akhir resolver yang berbeda, log kueri hanya menampilkan ID titik akhir resolver terakhir yang digunakan dalam rantai. Untuk melacak jalur resolusi lengkap melalui beberapa titik akhir, Anda dapat mengkorelasikan log di berbagai konfigurasi pencatatan kueri.

firewall_rule_group_id

ID grup aturan Firewall DNS yang cocok dengan nama domain dalam kueri. Ini diisi hanya jika Firewall DNS menemukan kecocokan untuk aturan dengan tindakan yang diatur ke pemberitahuan atau blokir.

Untuk informasi selengkapnya tentang grup aturan firewall, lihat [Grup aturan dan aturan DNS Firewall](#).

firewall_rule_action

Tindakan yang ditentukan oleh aturan yang cocok dengan nama domain dalam kueri. Ini diisi hanya jika Firewall DNS menemukan kecocokan untuk aturan dengan tindakan yang diatur ke pemberitahuan atau blokir.

firewall_domain_list_id

Daftar domain yang digunakan oleh aturan yang cocok dengan nama domain dalam kueri. Ini diisi hanya jika Firewall DNS menemukan kecocokan untuk aturan dengan tindakan yang diatur ke pemberitahuan atau blokir.

additional_properties

Informasi tambahan tentang peristiwa pengiriman log. `is_delayed`: Jika ada penundaan pengiriman log.

Contoh log kueri Route 53 VPC Resolver

Berikut adalah contoh log kueri Resolver:

```
{
  "srcaddr": "4.5.64.102",
  "vpc_id": "vpc-7example",
  "answers": [
    {
      "Rdata": "203.0.113.9",
      "Type": "PTR",
      "Class": "IN"
    }
  ],
  "firewall_rule_group_id": "rslvr-frg-01234567890abcdef",
  "firewall_rule_action": "BLOCK",
  "query_name": "15.3.4.32.in-addr.arpa.",
  "firewall_domain_list_id": "rslvr-fdl-01234567890abcdef",
  "query_class": "IN",
  "srcids": {
    "instance": "i-0d15cd0d3example"
  },
  "rcode": "NOERROR",
  "query_type": "PTR",
  "transport": "UDP",
  "version": "1.100000",
  "account_id": "111122223333",
  "srcport": "56067",
  "query_timestamp": "2021-02-04T17:51:55Z",
  "region": "us-east-1"
}
```

Berbagi konfigurasi pencatatan kueri Resolver dengan akun lain AWS

Anda dapat membagikan konfigurasi pencatatan kueri yang Anda buat menggunakan satu AWS akun dengan AWS akun lain. Untuk berbagi konfigurasi, konsol Resolver VPC Route 53 terintegrasi dengan AWS Resource Access Manager. Untuk informasi lebih lanjut tentang Resource Access Manager, lihat [Panduan Pengguna Resource Access Manager](#).

Perhatikan hal-hal berikut:

Mengaitkan VPCs dengan konfigurasi pencatatan kueri bersama

Jika AWS akun lain telah berbagi satu atau beberapa konfigurasi dengan akun Anda, Anda dapat mengaitkannya VPCs dengan konfigurasi dengan cara yang sama seperti yang Anda kaitkan VPCs dengan konfigurasi yang Anda buat.

Menghapus atau membatalkan berbagi konfigurasi

Jika Anda berbagi konfigurasi dengan akun lain dan kemudian menghapus konfigurasi atau berhenti membagikannya, dan jika satu atau lebih VPCs dikaitkan dengan konfigurasi, Route 53 VPC Resolver berhenti mencatat kueri DNS yang berasal dari itu. VPCs

Jumlah maksimum konfigurasi pencatatan kueri dan VPCs yang dapat dikaitkan dengan konfigurasi

Ketika akun membuat konfigurasi dan membagikannya dengan satu atau lebih akun lain, jumlah maksimum VPCs yang dapat dikaitkan dengan konfigurasi diterapkan per akun. Misalnya, jika Anda memiliki 10.000 akun di organisasi, Anda dapat membuat konfigurasi pencatatan kueri di akun pusat dan membagikannya melalui AWS RAM untuk membagikannya ke akun organisasi. Akun organisasi kemudian akan mengaitkan konfigurasi dengan VPCs penghitungannya terhadap asosiasi VPC konfigurasi log kueri akun mereka per Wilayah AWS batas 100. Namun, jika semua VPCs berada dalam satu akun, maka batas layanan akun mungkin diperlukan untuk ditingkatkan.

Untuk kuota Resolver VPC saat ini, lihat. [Kuota pada Route 53 VPC Resolver](#)

Izin

Untuk berbagi aturan dengan AWS akun lain, Anda harus memiliki izin untuk menggunakan [PutResolverQueryLogConfigPolicy](#) tindakan tersebut.

Pembatasan pada AWS akun tempat aturan dibagikan

Akun yang dibagikan aturan tidak dapat mengubah atau menghapus aturan.

Penandaan

Hanya akun yang membuat aturan yang dapat menambahkan, menghapus, atau melihat tanda pada aturan.

Untuk melihat status berbagi aturan saat ini (termasuk akun yang membagikan aturan atau akun tempat aturan dibagikan), dan untuk berbagi aturan dengan akun lain, lakukan prosedur berikut.

Cara melihat status berbagi dan berbagi konfigurasi pencatatan kueri dengan akun AWS lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Di panel navigasi, pilih Pencatatan Kueri.
3. Pada bilah navigasi, pilih Wilayah tempat Anda membuat aturan.

Kolom Status berbagi menampilkan status berbagi aturan saat ini yang dibuat oleh akun saat ini atau yang dibagikan dengan akun saat ini:

- Tidak dibagikan: AWS Akun saat ini membuat aturan, dan aturan tidak dibagikan dengan akun lain.
 - Dibagikan oleh saya: Akun saat ini membuat aturan dan membagikannya dengan satu atau beberapa akun.
 - Dibagikan dengan saya: Akun saat ini membuat aturan dan membagikannya dengan akun saat ini.
4. Pilih nama aturan dengan informasi berbagi yang ingin Anda tampilkan atau yang ingin Anda bagikan dengan akun lain.

Pada *rule name* halaman Aturan:, nilai di bawah Pemilik menampilkan ID akun yang membuat aturan. Itu adalah akun saat ini kecuali nilai Status berbagi adalah Dibagikan dengan saya. Dalam hal ini, Pemilik adalah akun yang membuat aturan dan membagikannya dengan akun saat ini.

Status berbagi juga ditampilkan.

5. Pilih Bagikan konfigurasi untuk membuka AWS RAM konsol
6. Untuk membuat pembagian sumber daya, ikuti langkah-langkah dalam [Membuat berbagi sumber daya di AWS RAM](#) dalam panduan AWS RAM pengguna.

 Note

Anda tidak dapat memperbarui pengaturan berbagi. Jika ingin mengubah salah satu pengaturan berikut, Anda harus membagikan ulang aturan dengan pengaturan baru lalu menghapus pengaturan berbagi yang lama.

Memantau pendaftaran domain

Dasbor Amazon Route 53 menyediakan informasi detail tentang status pendaftaran domain Anda, termasuk hal berikut:

- Status pendaftaran domain baru
- Status transfer domain ke Route 53
- Daftar domain yang mendekati tanggal kedaluwarsa

Kami merekomendasikan agar Anda memeriksa dasbor di konsol Route 53 secara berkala, terutama setelah Anda mendaftarkan domain baru atau mentransfer domain ke Route 53, untuk mengonfirmasi bahwa tidak ada masalah yang harus Anda tangani.

Kami juga menyarankan agar Anda mengonfirmasi bahwa informasi kontak untuk domain Anda sudah terbaru. Saat tanggal kedaluwarsa domain mendekat, kami mengirimkan email kepada kontak pendaftar domain tersebut dengan informasi tentang kapan domain kedaluwarsa dan cara memperbaruinya.

Memantau sumber daya Anda dengan pemeriksaan kesehatan Amazon Route 53 dan Amazon CloudWatch

Anda dapat memantau sumber daya Anda dengan membuat pemeriksaan kesehatan Amazon Route 53, yang digunakan CloudWatch untuk mengumpulkan dan memproses data mentah menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini dicatat dalam jangka waktu dua minggu, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa sumber daya Anda. Secara default, data metrik untuk pemeriksaan kesehatan Route 53 secara otomatis dikirim ke CloudWatch interval satu menit.

Untuk informasi selengkapnya tentang pemeriksaan kondisi Route 53, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#). Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) di Panduan CloudWatch Pengguna Amazon.

Metrik dan dimensi untuk pemeriksaan kondisi Route 53

Saat Anda membuat pemeriksaan kesehatan, Amazon Route 53 mulai mengirim metrik dan dimensi satu menit sekali ke CloudWatch sumber daya yang Anda tentukan. Konsol Route 53 memungkinkan Anda melihat status pemeriksaan kondisi. Anda juga dapat menggunakan prosedur berikut untuk

melihat metrik di CloudWatch konsol atau melihatnya menggunakan AWS Command Line Interface (AWS CLI).

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. Pada tab Semua metrik, pilih Route 53.
4. Pilih Metrik Pemeriksaan Kondisi.

Untuk melihat metrik menggunakan AWS CLI

- Pada prompt perintah, gunakan perintah berikut:

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Topik

- [CloudWatch metrik untuk pemeriksaan kesehatan Route 53](#)
- [Dimensi untuk metrik pemeriksaan kondisi Route 53](#)

CloudWatch metrik untuk pemeriksaan kesehatan Route 53

Namespace AWS/Route53 mencakup metrik pemeriksaan status kondisi Route 53 berikut.

ChildHealthCheckHealthyCount

Untuk pemeriksaan kesehatan yang diperhitungkan, jumlah pemeriksaan kesehatan yang sehat.

Statistik yang valid: Rata-rata (direkomendasikan), Minimum, Maksimum

Unit: Hitungan

ConnectionTime

Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksa kondisi Route 53 untuk membuat koneksi TCP dengan titik akhir. Anda dapat melihat ConnectionTime untuk pemeriksaan kondisi di seluruh wilayah atau untuk wilayah geografis yang dipilih.

Statistik yang valid: Rata-rata (direkomendasikan), Minimum, Maksimum

Unit: Milidetik

HealthCheckPercentageHealthy

Persentase pemeriksaan kondisi Route 53 yang menganggap titik akhir yang dipilih sebagai sehat.

Statistik yang valid: Rata-rata, Minimum, Maksimum

Unit: Persen

HealthCheckStatus

Status titik akhir pemeriksaan kesehatan yang CloudWatch sedang diperiksa. 1 menunjukkan sehat, dan 0 menunjukkan tidak sehat.

Statistik yang valid: Minimum, Rata-rata, dan Maksimum

Unit: tidak ada

SSLHandshakeWaktu

Rata-rata waktu, dalam milidetik, yang dibutuhkan oleh pemeriksaan kondisi Route 53 untuk menyelesaikan handshake SSL. Anda dapat melihat `SSLHandshakeTime` untuk pemeriksaan kondisi di seluruh wilayah atau untuk wilayah geografis yang dipilih.

Statistik yang valid: Rata-rata (direkomendasikan), Minimum, Maksimum

Unit: Milidetik

TimeToFirstByte

Rata-rata waktu, dalam milidetik, yang dibutuhkan pemeriksaan kondisi Route 53 untuk menerima byte pertama respons bagi permintaan HTTP atau HTTPS. Anda dapat melihat `TimeToFirstByte` untuk pemeriksaan kondisi di seluruh wilayah atau untuk wilayah geografis yang dipilih.

Statistik yang valid: Rata-rata (direkomendasikan), Minimum, Maksimum

Unit: Milidetik

Dimensi untuk metrik pemeriksaan kondisi Route 53

Metrik Route 53 untuk pemeriksaan kondisi menggunakan namespace `AWS/Route53` dan menyediakan metrik untuk `HealthCheckId`. Ketika mengambil metrik, Anda harus menyediakan dimensi `HealthCheckId`.

Selain itu, untuk `ConnectionTime`, `SSLHandshakeTime`, dan `TimeToFirstByte`, Anda dapat menentukan `Region` secara opsional. Jika Anda menghilangkan `Region`, CloudWatch mengembalikan metrik di semua wilayah. Jika Anda menyertakan `Region`, CloudWatch mengembalikan metrik hanya untuk wilayah tertentu.

Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

Memantau zona yang dihosting menggunakan Amazon CloudWatch

Anda dapat memantau zona yang dihosting publik dengan menggunakan Amazon CloudWatch untuk mengumpulkan dan memproses data mentah menjadi metrik yang dapat dibaca, mendekati waktu nyata. Metrik tersedia segera setelah Route 53 menerima kueri DNS yang menjadi dasar metrik. CloudWatch data metrik untuk zona yang dihosting Route 53 memiliki perincian satu menit.

Untuk informasi lebih lanjut, lihat dokumentasi berikut

- Untuk gambaran umum dan informasi tentang cara melihat metrik di CloudWatch konsol Amazon dan cara mengambil metrik menggunakan AWS Command Line Interface (AWS CLI), lihat [Melihat metrik kueri DNS untuk zona yang di-hosting publik](#)
- Untuk informasi tentang periode retensi metrik, lihat [GetMetricStatistics](#) di Referensi Amazon CloudWatch API.
- Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) di Panduan CloudWatch Pengguna Amazon.
- Untuk informasi selengkapnya tentang CloudWatch metrik, lihat [Menggunakan CloudWatch metrik Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Topik

- [CloudWatch metrik untuk Route 53 zona yang dihosting publik](#)
- [CloudWatch dimensi untuk metrik zona yang dihosting publik Route 53](#)

CloudWatch metrik untuk Route 53 zona yang dihosting publik

AWS/Route53Namespace menyertakan metrik berikut untuk zona yang dihosting Route 53:

DNSQueries

Untuk zona yang dihosting, jumlah kueri DNS yang ditanggapi Route 53 dalam periode waktu tertentu.

Statistik yang valid: Jumlah, SampleCount

Unit: Hitungan

Wilayah: Route 53 adalah layanan global. Untuk mendapatkan metrik zona yang di-hosting, Anda harus menentukan US East (N. Virginia) sebagai Wilayah.

DNSSECInternalKegagalan

Nilai adalah 1 jika ada objek di zona yang di-hosting dalam status INTERNAL_FAILURE. Jika tidak, nilai adalah 0.

Statistik yang valid: Jumlah

Unit: Hitungan

Volume: 1 per 4 jam per zona yang dihosting

Wilayah: Route 53 adalah layanan global. Untuk mendapatkan metrik zona yang di-hosting, Anda harus menentukan US East (N. Virginia) sebagai Wilayah.

DNSSECKeySigningKeysNeedingAction

Jumlah kunci penandatanganan kunci (KSKs) yang memiliki status ACTION_NEEDED (karena kegagalan KMS).

Statistik yang valid: Jumlah, SampleCount

Unit: Hitungan

Volume: 1 per 4 jam per zona yang dihosting

Wilayah: Route 53 adalah layanan global. Untuk mendapatkan metrik zona yang di-hosting, Anda harus menentukan US East (N. Virginia) sebagai Wilayah.

DNSSECKeySigningKeyMaxNeedingActionAge

Waktu sejak kunci penandatanganan kunci (KSK) diatur ke status ACTION_NEEDED.

Statistik yang valid: Maksimum

Unit: detik

Volume: 1 per 4 jam per zona yang dihosting

Wilayah: Route 53 adalah layanan global. Untuk mendapatkan metrik zona yang di-hosting, Anda harus menentukan US East (N. Virginia) sebagai Wilayah.

DNSSECKeySigningKeyAge

Waktu sejak kunci penandatanganan kunci (KSK) dibuat (bukan sejak diaktifkan).

Statistik yang valid: Maksimum

Unit: detik

Volume: 1 per 4 jam per zona yang dihosting

Wilayah: Route 53 adalah layanan global. Untuk mendapatkan metrik zona yang di-hosting, Anda harus menentukan US East (N. Virginia) sebagai Wilayah.

CloudWatch dimensi untuk metrik zona yang dihosting publik Route 53

Metrik Route 53 untuk zona yang di-hosting menggunakan namespace `AWS/Route53` dan menyediakan metrik untuk `HostedZoneId`. Untuk mendapatkan jumlah kueri DNS, Anda harus menentukan ID zona yang di-hosting dalam dimensi `HostedZoneId`.

Memantau Route 53 titik akhir VPC Resolver dengan Amazon CloudWatch

Anda dapat menggunakan Amazon CloudWatch untuk memantau jumlah kueri DNS yang diteruskan oleh titik akhir Route 53 VPC Resolver. Amazon CloudWatch mengumpulkan dan memproses data mentah menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini dicatat dalam jangka waktu dua minggu, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa sumber daya Anda. Secara default, data metrik untuk titik akhir Resolver secara otomatis dikirim ke CloudWatch interval lima menit. Interval lima menit juga merupakan interval terkecil di mana data metrik dapat dikirim.

Untuk informasi selengkapnya tentang VPC Resolver, lihat [Apa itu Route 53 VPC Resolver?](#) Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) di Panduan CloudWatch Pengguna Amazon.

Metrik dan dimensi untuk Route 53 VPC Resolver

Saat Anda mengonfigurasi VPC Resolver untuk meneruskan kueri DNS ke jaringan Anda atau sebaliknya, VPC Resolver mulai mengirim [metrik](#) dan [dimensi](#) setiap lima menit sekali ke sekitar jumlah kueri yang diteruskan. CloudWatch Anda dapat menggunakan prosedur berikut untuk melihat metrik di CloudWatch konsol atau melihatnya menggunakan AWS Command Line Interface (AWS CLI).

Untuk melihat metrik VPC Resolver menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada bilah navigasi, pilih Wilayah tempat Anda membuat titik akhir.
3. Pada panel navigasi, silakan pilih Metrik.
4. Pada tab Semua metrik, pilih Route 53 Resolver.
5. Pilih Menurut Titik Akhir untuk melihat jumlah kueri titik akhir tertentu. Kemudian pilih titik akhir yang ingin Anda lihat jumlah kuerinya.

Pilih Di Seluruh Semua Titik Akhir untuk melihat jumlah kueri untuk semua titik akhir masuk atau untuk semua titik akhir keluar yang dibuat oleh akun saat ini. AWS Kemudian pilih InboundQueryVolumeatau OutboundQueryVolumeuntuk melihat jumlah yang diinginkan.

Untuk melihat metrik menggunakan AWS CLI

- Pada prompt perintah, gunakan perintah berikut:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Topik

- [CloudWatch Metrik Dasar untuk Route 53 VPC Resolver](#)
- [CloudWatch Metrik Terperinci untuk Route 53 VPC Resolver](#)
- [Dimensi untuk metrik Route 53 VPC Resolver](#)

CloudWatch Metrik Dasar untuk Route 53 VPC Resolver

AWS/Route53Resolvernamespace mencakup metrik dasar untuk titik akhir Route 53 VPC Resolver dan untuk alamat IP tanpa biaya.

Topik

- [Metrik untuk titik akhir Route 53 VPC Resolver](#)
- [Metrik untuk alamat IP Route 53 VPC Resolver](#)

Metrik untuk titik akhir Route 53 VPC Resolver

AWS/Route53ResolverNamespace menyertakan metrik berikut untuk titik akhir Route 53 VPC Resolver.

EndpointHealthyENICount

Jumlah antarmuka jaringan elastis dalam status OPERATIONAL. Ini berarti bahwa antarmuka jaringan VPC Amazon untuk titik akhir (ditentukan oleh `EndpointId`) dikonfigurasi dengan benar dan dapat meneruskan kueri DNS masuk atau keluar antara jaringan Anda dan Resolver.

Statistik yang Valid: Minimum, Maksimum, Rata-rata

Unit: Hitungan

EndpointUnhealthyENICount

Jumlah antarmuka jaringan elastis dalam status AUTO_RECOVERING.

Ini berarti penyelesaian mencoba memulihkan satu atau beberapa antarmuka jaringan Amazon VPC yang terkait dengan titik akhir (ditentukan oleh `EndpointId`). Selama proses pemulihan, titik akhir berfungsi dengan kapasitas terbatas dan tidak dapat memproses kueri DNS hingga sepenuhnya pulih.

Statistik yang Valid: Minimum, Maksimum, Rata-rata

Unit: Hitungan

InboundQueryVolume

Untuk titik akhir masuk, jumlah kueri DNS yang diteruskan dari jaringan Anda ke Anda VPCs melalui titik akhir yang ditentukan oleh `EndpointId`

Statistik Valid: Sum

Unit: Hitungan

OutboundQueryVolume

Untuk titik akhir keluar, jumlah kueri DNS yang diteruskan dari jaringan Anda VPCs ke jaringan Anda melalui titik akhir yang ditentukan oleh. `EndpointId`

Statistik Valid: Sum

Unit: Hitungan

OutboundQueryAggregateVolume

Untuk titik akhir keluar, jumlah total kueri DNS yang diteruskan dari Amazon VPCs ke jaringan Anda, termasuk yang berikut ini:

- Jumlah kueri DNS yang diteruskan dari Anda VPCs ke jaringan Anda melalui titik akhir yang ditentukan oleh. `EndpointId`
- Ketika akun saat ini membagikan aturan Resolver dengan akun lain, kueri dari akun VPCs tersebut dibuat oleh akun lain yang diteruskan ke jaringan Anda melalui titik akhir yang ditentukan oleh. `EndpointId`

Statistik Valid: Sum

Unit: Hitungan

ResolverEndpointCapacityStatus

Status kapasitas titik akhir Resolver. Metrik menunjukkan keadaan pemanfaatan kapasitas saat ini di mana: 0 = OK (Kapasitas operasi normal), 1 = Peringatan (Setidaknya satu elastic network interface melebihi 50% pemanfaatan kapasitas), dan 2 = Kritis (Setidaknya satu elastic network interface melebihi 75% pemanfaatan kapasitas).

Status kapasitas ditentukan oleh beberapa faktor termasuk volume kueri, latensi kueri, protokol DNS, ukuran paket DNS, dan status pelacakan koneksi.

Statistik yang Valid: Maksimum

Satuan: Tidak ada

Praktik terbaik untuk Manajemen Kapasitas Titik Akhir VPC Resolver

Untuk mengatasi masalah kapasitas, kami biasanya menyarankan untuk meningkatkan jumlah antarmuka jaringan elastis untuk titik akhir Resolver Anda. Namun, ada pertimbangan penting untuk jenis titik akhir tertentu:

Untuk titik akhir masuk, penyeimbangan beban lalu lintas bergantung pada pelanggan. Oleh karena itu peringatan kapasitas atau peringatan kritis dapat menunjukkan “hot spot” di mana subset antarmuka jaringan elastis digunakan secara tidak proporsional.

- Untuk mengidentifikasi potensi masalah load balancing, periksa [InboundQueryVolume](#) metrik untuk setiap elastic network interface secara individual.

Untuk titik akhir keluar, lalu lintas secara otomatis diseimbangkan di seluruh antarmuka jaringan elastis. Masalah kapasitas mungkin disebabkan oleh masalah dengan server nama target, atau karena permintaan batas waktu latensi tinggi membanjiri antarmuka jaringan Resolver.

- Dalam kasus ini, hanya meningkatkan antarmuka jaringan elastis mungkin tidak efektif, dan kami sarankan untuk memperbaiki server nama target.

Metrik untuk alamat IP Route 53 VPC Resolver

Namespace `AWS/Route53Resolver` menyertakan metrik berikut untuk setiap alamat IP yang terkait dengan titik akhir masuk atau keluar Resolver. (Saat Anda menentukan titik akhir, VPC Resolver membuat antarmuka jaringan [elastis Amazon VPC](#).)

InboundQueryVolume

Untuk setiap alamat IP titik akhir masuk Anda, jumlah kueri DNS yang diteruskan dari jaringan ke alamat IP yang ditentukan. Setiap alamat IP diidentifikasi oleh ID alamat IP. Anda bisa mendapatkan nilai ini menggunakan konsol Route 53. Pada halaman untuk titik akhir yang berlaku, di bagian alamat IP, lihat kolom ID alamat IP. Anda juga bisa mendapatkan nilai secara terprogram menggunakan [ListResolverEndpointIpAddresses](#)

Statistik Valid: Sum

Unit: Hitungan

OutboundQueryAggregateVolume

Untuk setiap alamat IP untuk titik akhir keluar Anda, jumlah total kueri DNS yang diteruskan dari Amazon VPCs ke jaringan Anda, termasuk yang berikut ini:

- Jumlah kueri DNS yang diteruskan dari Anda VPCs ke jaringan Anda menggunakan alamat IP yang ditentukan.

- Ketika akun saat ini membagikan aturan Resolver dengan akun lain, kueri dari akun VPCs tersebut dibuat oleh akun lain yang diteruskan ke jaringan Anda melalui penggunaan alamat IP yang ditentukan.

Setiap alamat IP diidentifikasi oleh ID alamat IP. Anda bisa mendapatkan nilai ini menggunakan konsol Route 53. Pada halaman untuk titik akhir yang berlaku, di bagian alamat IP, lihat kolom ID alamat IP. Anda juga bisa mendapatkan nilai secara terprogram menggunakan.

[ListResolverEndpointIpAddresses](#)

Statistik Valid: Sum

Unit: Hitungan

CloudWatch Metrik Terperinci untuk Route 53 VPC Resolver

Route 53 VPC Resolver menyediakan RNI Enhanced dan Target Name Server Metrics sebagai fitur pilihan untuk titik akhir. Metrik ini dikirim ke CloudWatch interval 1 menit.

Note

- Metrik terperinci tidak diaktifkan secara default, tetapi dapat diaktifkan pada tingkat titik akhir. Metrik ini dapat diaktifkan secara terprogram saat membuat atau memperbarui titik akhir menggunakan tanda dan. `RniEnhancedMetricsEnabled` `TargetNameServerMetricsEnabled` Untuk informasi selengkapnya, lihat [CreateResolverEndpoint](#) dan [UpdateResolverEndpoint](#).
- CloudWatch Harga dan biaya standar diterapkan untuk menggunakan metrik rinci titik akhir Route 53 Resolver. Untuk informasi selengkapnya, lihat [CloudWatch Harga Amazon](#).

Topik

- [Metrik yang Ditingkatkan RNI](#)
- [Metrik Server Nama Target](#)

Metrik yang Ditingkatkan RNI

Route 53 Resolver menerbitkan metrik yang disempurnakan RNI ke Amazon CloudWatch untuk memantau kinerja dan kesehatan titik akhir Resolver dan alamat IP Resolver. AWS/

Route53ResolverNamespace mencakup metrik yang ditingkatkan RNI berikut untuk titik akhir masuk dan keluar Resolver Route 53 Resolver di, dimensi: EndpointId RniId

P90 ResponseTime

Latensi respons persentil ke-90 dari kueri DNS yang diterima oleh IP Resolver () yang terkait dengan titik akhir Resolver () RniId EndpointId

Statistik yang Valid: Maksimum

Unit: Mikrodetik

ServFailQueries

Jumlah respons SERVFAIL untuk kueri DNS yang dikirim ke IP Resolver () yang terkait dengan titik akhir Resolver (RniId) EndpointId

Statistik Valid: Sum

Unit: Hitungan

NxDomainQueries

Jumlah respons NXDOMAIN untuk kueri DNS yang dikirim ke IP Resolver () yang terkait dengan titik akhir Resolver (RniId) EndpointId

Statistik Valid: Sum

Unit: Hitungan

RefusedQueries

Jumlah tanggapan YANG DITOLAK untuk kueri DNS yang dikirim ke IP Resolver () yang terkait dengan titik akhir Resolver (RniId) EndpointId

Statistik Valid: Sum

Unit: Hitungan

FormErrorQueries

Jumlah tanggapan FORMERR untuk kueri DNS yang dikirim ke IP Resolver () yang terkait dengan titik akhir Resolver (RniId) EndpointId

Statistik Valid: Sum

Unit: Hitungan

TimeoutQueries

Jumlah batas waktu untuk kueri DNS yang dikirim ke IP Resolver () yang terkait dengan titik akhir Resolver (RniId) EndpointId

Statistik Valid: Sum

Unit: Hitungan

Metrik Server Nama Target

Route 53 Resolver menerbitkan metrik server nama target ke CloudWatch Amazon untuk memantau kinerja dan ketersediaan server nama target yang terkait dengan titik akhir Resolver. AWS/Route53ResolverNamespace menyertakan metrik terperinci berikut untuk titik akhir keluar Route 53 Resolver dalam dimensi: EndpointID TargetNameServerIP

P90 ResponseTime

Latensi respons persentil ke-90 dari Target Name Server IP (TargetNameServerIP) untuk kueri DNS yang dikirim melalui titik akhir Resolver () EndpointID

Statistik yang Valid: Maksimum

Unit: Mikrodetik

RequestQueries

Jumlah kueri DNS yang dikirim ke IP Server Nama Target (TargetNameServerIP) melalui titik akhir Resolver (). EndpointID

Statistik Valid: Sum

Unit: Hitungan

TimeoutQueries

Jumlah kueri DNS yang dikirim melalui titik akhir Resolver (EndpointID) yang habis waktunya di IP Server Nama Target (). TargetNameServerIP

Statistik Valid: Sum

Unit: Hitungan

Note

Dalam beberapa kasus, kesenjangan dapat diamati dalam metrik VPC Resolver (ResolverEndpointCapacityStatus) dan metrik yang ditingkatkan RNI. Kesenjangan ini dapat terjadi ketika antarmuka jaringan Anda menjalani pemeliharaan atau pembaruan terjadwal berturut-turut. Setelah kami mengembalikan antarmuka jaringan ke layanan, dibutuhkan setidaknya 1 menit bagi layanan kami untuk mengumpulkan data operasional dan mempublikasikan metrik ini. Kesenjangan ini tidak menunjukkan bahwa titik akhir VPC Resolver Anda mengalami pemadaman. Jika Anda mengonfigurasi CloudWatch alarm untuk metrik ini, kami merekomendasikan hal berikut:

- Atur alarm ke “Perlakukan data yang hilang sebagai abaikan”, atau
- Konfigurasi periode evaluasi lebih dari lima menit untuk ambang alarm.

Pengaturan ini akan membantu mengurangi alarm palsu selama aktivitas pemeliharaan normal.

Dimensi untuk metrik Route 53 VPC Resolver

Metrik Route 53 VPC Resolver untuk titik akhir masuk dan keluar menggunakan AWS/Route53Resolver namespace dan menyediakan metrik untuk dimensi berikut:

- `EndpointId`: Jika Anda menentukan nilai untuk `EndpointId` dimensi, CloudWatch mengembalikan jumlah query DNS untuk titik akhir yang ditentukan. Jika Anda tidak menentukan `EndpointId`, CloudWatch mengembalikan jumlah kueri DNS untuk semua titik akhir yang dibuat oleh akun saat ini. AWS
- `RniId` dimensi didukung untuk `OutboundQueryAggregateVolume` dan `InboundQueryVolume` metrik.
- `EndpointId`, `RniId` dimensi didukung untuk `P90ResponseTime`, `ServFailQueries`, `NxDomainQueries`, `RefusedQueries`, `FormErrorQueries`, dan `TimeoutQueries` untuk Alamat IP Resolver yang terkait dengan titik akhir resolver.

- EndpointID, TargetNameServerIP dimensi didukung untukP90ResponseTime,RequestQueries, dan TimeoutQueries untuk server nama target yang terkait dengan titik akhir resolver.

Memantau grup aturan DNS Firewall Resolver dengan Amazon CloudWatch

Anda dapat menggunakan Amazon CloudWatch untuk memantau jumlah kueri DNS yang difilter oleh grup aturan Resolver DNS Firewall. Amazon CloudWatch mengumpulkan dan memproses data mentah menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini dicatat dalam jangka waktu dua minggu, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa sumber daya Anda. Secara default, data metrik untuk grup aturan DNS Firewall dikirim secara otomatis CloudWatch pada interval lima menit.

Untuk informasi selengkapnya tentang Firewall DNS, lihat [Menggunakan DNS Firewall untuk menyaring lalu lintas DNS keluar](#). Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) di Panduan CloudWatch Pengguna Amazon.

Metrik dan dimensi untuk Resolver DNS Firewall

Saat Anda mengaitkan grup aturan Resolver DNS Firewall dengan VPC untuk memfilter kueri DNS, DNS Firewall mulai mengirim metrik dan dimensi setiap 5 menit sekali ke kueri yang difilter. CloudWatch Untuk informasi tentang metrik dan dimensi Firewall DNS, lihat [CloudWatch metrik untuk Resolver DNS Firewall](#).

Anda dapat menggunakan prosedur berikut untuk melihat metrik di CloudWatch konsol atau melihatnya menggunakan AWS Command Line Interface (AWS CLI).

Untuk melihat metrik DNS Firewall menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di bilah navigasi, pilih Wilayah yang ingin Anda lihat.
3. Pada panel navigasi, silakan pilih Metrik.
4. Pada tab Semua metrik, pilih Route 53 VPC Resolver.
5. Pilih metrik yang menarik bagi Anda.

Untuk melihat metrik menggunakan AWS CLI

- Pada prompt perintah, gunakan perintah berikut:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Topik

- [CloudWatch metrik untuk Resolver DNS Firewall](#)

CloudWatch metrik untuk Resolver DNS Firewall

AWS/Route53ResolverNamespace menyertakan metrik untuk grup aturan Resolver DNS Firewall.

Topik

- [Metrik untuk grup aturan Resolver DNS Firewall](#)
- [Metrik untuk VPCs](#)
- [Metrik untuk grup aturan firewall dan pengaitan VPC](#)
- [Metrik untuk daftar domain di grup aturan firewall](#)

Metrik untuk grup aturan Resolver DNS Firewall

FirewallRuleGroupQueryVolume

Jumlah kueri Firewall DNS yang cocok dengan grup aturan firewall (ditentukan oleh FirewallRuleGroupId).

Dimensi: FirewallRuleGroupId

Statistik yang valid: Jumlah

Unit: Hitungan

Metrik untuk VPCs

VpcFirewallQueryVolume

Jumlah kueri Firewall DNS dari VPC (ditentukan oleh VpcId).

Dimensi: VpcId

Statistik yang valid: Jumlah

Unit: Hitungan

Metrik untuk grup aturan firewall dan pengaitan VPC

FirewallRuleGroupVpcQueryVolume

Jumlah kueri Firewall DNS dari VPC (ditentukan oleh VpcId) yang cocok dengan grup aturan firewall (ditentukan oleh FirewallRuleGroupId).

Dimensi: FirewallRuleGroupId, VpcId

Statistik yang valid: Jumlah

Unit: Hitungan

Metrik untuk daftar domain di grup aturan firewall

FirewallRuleQueryVolume

Jumlah kueri firewall DNS yang cocok dengan daftar domain firewall (ditentukan oleh FirewallDomainListId) dalam grup aturan firewall (ditentukan oleh FirewallRuleGroupId).

Dimensi: FirewallRuleGroupId, FirewallDomainListId

Statistik yang valid: Jumlah

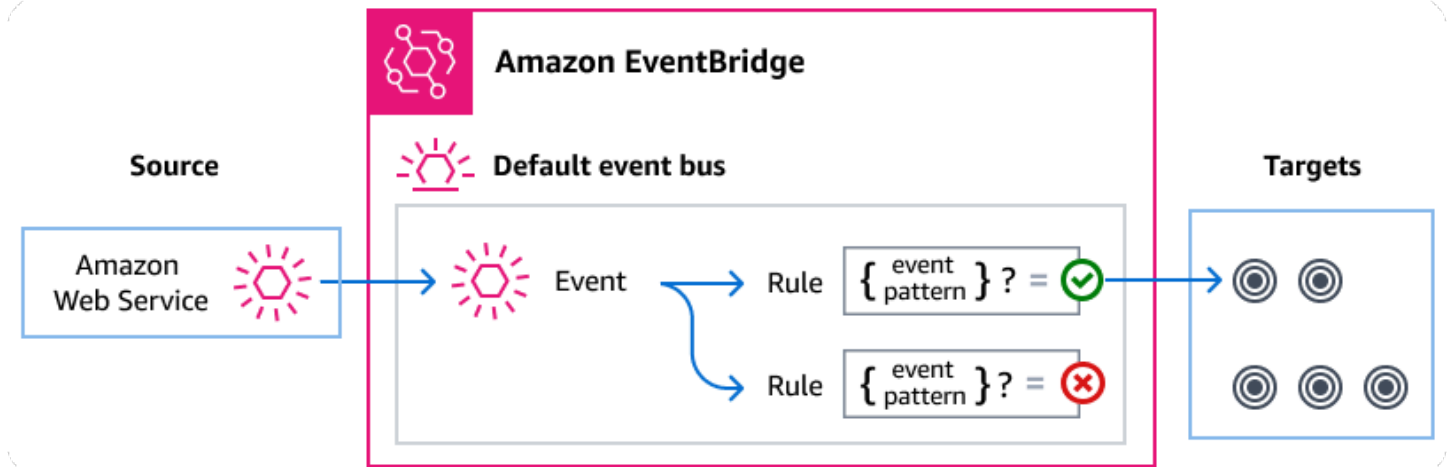
Unit: Hitungan

Mengelola peristiwa Resolver DNS Firewall menggunakan Amazon EventBridge

Amazon EventBridge adalah layanan tanpa server yang menggunakan peristiwa untuk menghubungkan komponen aplikasi bersama-sama, sehingga memudahkan Anda untuk membangun aplikasi berbasis peristiwa yang dapat diskalakan. Arsitektur berbasis peristiwa adalah gaya membangun sistem perangkat lunak yang digabungkan secara longgar yang bekerja sama

dengan memancarkan dan menanggapi peristiwa. Peristiwa mewakili perubahan dalam sumber daya atau lingkungan.

Seperti banyak AWS layanan, DNS Firewall menghasilkan dan mengirim acara ke bus acara EventBridge default. (Bus acara default secara otomatis disediakan di setiap AWS akun.) Bus acara adalah router yang menerima acara dan mengirimkannya ke nol atau lebih tujuan, atau target. Aturan yang Anda tentukan untuk bus acara mengevaluasi peristiwa saat mereka tiba. Setiap aturan memeriksa apakah suatu peristiwa cocok dengan pola acara aturan. Jika acara tidak cocok, bus acara mengirimkan acara ke target yang ditentukan.



Topik

- [Acara Resolver DNS Firewall](#)
- [Mengirim peristiwa Resolver DNS Firewall menggunakan aturan EventBridge](#)
- [Amazon EventBridge izin](#)
- [EventBridge Sumber daya tambahan](#)
- [Referensi detail acara Resolver DNS Firewall](#)

Acara Resolver DNS Firewall

VPC Resolver mengirimkan peristiwa DNS Firewall ke bus acara default secara otomatis.

EventBridge Anda dapat membuat aturan di bus acara; setiap aturan mencakup pola acara dan satu atau lebih target. Peristiwa yang cocok dengan pola acara aturan dikirimkan ke target yang ditentukan [berdasarkan upaya terbaik](#). Acara mungkin dikirim rusak.

Peristiwa berikut dihasilkan oleh DNS Firewall. Untuk informasi selengkapnya, lihat [EventBridge](#) di Panduan Amazon EventBridge Pengguna. .

Jenis detail acara	Deskripsi
Blok Firewall DNS	Tindakan blok apa pun yang dilakukan pada domain.
Peringatan Firewall DNS	Tindakan peringatan apa pun yang dilakukan pada domain.

Mengirim peristiwa Resolver DNS Firewall menggunakan aturan EventBridge

Agar bus acara EventBridge default mengirim peristiwa DNS Firewall ke target, Anda harus membuat aturan yang berisi pola peristiwa yang cocok dengan data dalam peristiwa DNS Firewall yang diinginkan.

Membuat aturan terdiri dari langkah-langkah umum berikut:

1. Membuat pola acara untuk aturan yang menentukan:
 - VPC Resolver adalah sumber peristiwa yang dievaluasi oleh aturan.
 - (Opsional): Setiap data acara lain untuk dicocokkan.

Untuk informasi selengkapnya, lihat [???](#)

2. (Opsional): Membuat transformator input yang menyesuaikan data dari peristiwa sebelum EventBridge meneruskan informasi ke target aturan.

Untuk informasi selengkapnya, lihat [Transformasi input](#) di Panduan EventBridge Pengguna.

3. Menentukan target yang ingin EventBridge Anda sampaikan acara yang cocok dengan pola acara.

Target dapat berupa AWS layanan lain, aplikasi software-as-a-service (SaaS), tujuan API, atau titik akhir khusus lainnya. Untuk informasi lebih lanjut, lihat [Target](#) di Panduan Pengguna EventBridge .

Untuk petunjuk komprehensif tentang cara membuat aturan bus acara, lihat [Membuat aturan yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna.

Membuat pola acara untuk acara Resolver DNS Firewall

Saat DNS Firewall mengirimkan peristiwa ke bus peristiwa default, EventBridge gunakan pola peristiwa yang ditentukan untuk setiap aturan untuk menentukan apakah acara harus dikirim ke target

aturan. Pola peristiwa cocok dengan data dalam peristiwa DNS Firewall yang diinginkan. Setiap pola acara adalah objek JSON yang berisi:

- `source` Atribut yang mengidentifikasi layanan yang mengirim acara. Untuk acara DNS Firewall, sumbernya adalah `aws.route53resolver`.
- (Opsional): `detail-type` Atribut yang berisi array jenis acara yang cocok.
- (Opsional): `detail` Atribut yang berisi data acara lain yang cocok.

Misalnya, pola peristiwa berikut cocok dengan peristiwa peringatan dan pemblokiran dari DNS Firewall:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

Sedangkan pola event berikut cocok dengan aksi BLOCK:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS Firewall mengirimkan acara yang sama untuk domain yang sama hanya sekali dalam jendela 6 jam. Contoh:

1. Instance i-123 mengirim kueri DNS `exampledomain.com` pada waktu T1. DNS Firewall mengirimkan peringatan atau peristiwa pemblokiran karena ini adalah kejadian pertama.
2. Instance i-123 mengirim DNSQuery `exampledomain.com` pada waktu T1+30 menit. DNS Firewall tidak mengirim peringatan atau memblokir peristiwa karena ini adalah kejadian berulang dalam jendela 6 jam.
3. Instance i-123 mengirim kueri DNS `exampledomain.com` pada waktu T1+7 jam. DNS Firewall mengirimkan peringatan atau peristiwa pemblokiran karena ini terjadi di luar jendela 6 jam.

Untuk informasi selengkapnya tentang penulisan pola acara, lihat [Pola acara](#) di Panduan EventBridge Pengguna.

Menguji pola acara untuk acara DNS Firewall di EventBridge

Anda dapat menggunakan EventBridge Sandbox untuk mendefinisikan dan menguji pola peristiwa dengan cepat, tanpa harus menyelesaikan proses pembuatan atau pengeditan aturan yang lebih besar. Menggunakan Sandbox, Anda dapat menentukan pola peristiwa dan menggunakan contoh peristiwa untuk mengonfirmasi pola cocok dengan peristiwa yang diinginkan. EventBridge memberi Anda pilihan untuk membuat aturan baru menggunakan pola acara itu, langsung dari kotak pasir.

Untuk informasi selengkapnya, lihat [Menguji pola peristiwa menggunakan EventBridge Kotak Pasir](#) di Panduan EventBridge Pengguna.

Membuat EventBridge aturan dan target untuk DNS Firewall

Prosedur berikut menunjukkan cara membuat aturan yang memungkinkan EventBridge untuk mengirim peristiwa untuk semua peringatan DNS Firewall dan tindakan blok, dan menambahkan AWS Lambda fungsi sebagai target untuk aturan tersebut.

1. Gunakan AWS CLI untuk membuat EventBridge aturan:

```
aws events put-rule \  
--event-pattern "{\"source\":  
[\"aws.route53resolver\"],\"detail-type\":  
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \  
--name dns-firewall-rule
```

2. Lampirkan fungsi Lambda sebagai target aturan:

```
AWS events put-targets --rule dns-firewall-rule --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. Untuk menambahkan izin yang diperlukan untuk memanggil target, jalankan perintah Lambda berikut: AWS CLI

```
AWS lambda add-permission --function-name <your_function> --statement-  
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge izin

DNS Firewall tidak memerlukan izin tambahan untuk mengirimkan acara ke Amazon EventBridge

Target yang Anda tentukan mungkin memerlukan izin atau konfigurasi tertentu. Untuk detail selengkapnya tentang penggunaan layanan khusus untuk target, lihat [Amazon EventBridge target](#) di Panduan Amazon EventBridge Pengguna.

EventBridge Sumber daya tambahan

Lihat topik-topik berikut di [Panduan Amazon EventBridge Pengguna](#) untuk informasi lebih lanjut tentang cara menggunakan EventBridge untuk memproses dan mengelola acara.

- Untuk informasi rinci tentang cara kerja bus acara, lihat [bus Amazon EventBridge acara](#).
- Untuk informasi tentang struktur acara, lihat [Acara](#).
- Untuk informasi tentang membuat pola peristiwa untuk EventBridge digunakan saat mencocokkan peristiwa dengan aturan, lihat [Pola acara](#).
- Untuk informasi tentang membuat aturan untuk menentukan EventBridge proses peristiwa, lihat [Aturan](#).
- Untuk informasi tentang menentukan layanan atau tujuan lain yang EventBridge mengirimkan peristiwa yang cocok, lihat [Target](#).

Referensi detail acara Resolver DNS Firewall

Semua peristiwa dari AWS layanan memiliki seperangkat bidang umum yang berisi metadata tentang acara tersebut, seperti AWS layanan yang merupakan sumber acara, waktu acara dibuat, akun dan wilayah tempat acara berlangsung, dan lainnya. Untuk definisi bidang umum ini, lihat [Referensi struktur acara](#) di Panduan Amazon EventBridge Pengguna.

Selain itu, setiap acara memiliki detail bidang yang berisi data khusus untuk peristiwa tertentu. Referensi di bawah ini mendefinisikan bidang detail untuk berbagai peristiwa DNS Firewall.

Saat menggunakan EventBridge untuk memilih dan mengelola peristiwa DNS Firewall, penting untuk mengingat hal berikut:

- `sourceBidang` untuk semua peristiwa dari DNS Firewall diatur ke `aws.route53resolver`.
- `detail-typeBidang` menentukan jenis acara.

Misalnya, DNS Firewall Block atau DNS Firewall Alert.

- `detailBidang` berisi data yang spesifik untuk peristiwa tertentu.

Untuk informasi tentang membuat pola peristiwa yang memungkinkan aturan agar sesuai dengan peristiwa DNS Firewall, lihat [Pola acara](#) di Amazon EventBridge Panduan Pengguna.

Untuk informasi selengkapnya tentang peristiwa dan cara EventBridge memprosesnya, lihat [Amazon EventBridge peristiwa](#) di Panduan Amazon EventBridge Pengguna.

Topik

- [Detail acara peringatan DNS Firewall](#)
- [Detail acara blok DNS Firewall](#)

Detail acara peringatan DNS Firewall

Di bawah ini adalah bidang detail untuk detail acara status Peringatan.

detail-typeBidang source dan disertakan karena berisi nilai khusus untuk acara Route 53.

```
{...,
  "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
  ...,
  "detail": {
    "account-id": "string",
    "last-observed-at": "string",
    "query-name": "string",
    "query-type": "string",
    "query-class": "string",
    "transport": "string",
    "firewall-rule-action": "string",
    "firewall-rule-group-id": "string",
    "firewall-domain-list-id": "string",
    "firewall-protection": "string",
    "resources": [{
      "resource-type": "string",
      "instance-details": {
        "id": "string",
      }
    }],
  },
  {
    "resource-type": "string",
    "resolver-endpoint-details": {
      "id": "string"
    }
  }
}
```

```
}  
]
```

detail-type

Mengidentifikasi jenis acara.

Untuk acara ini, nilai ini adalah `DNS Firewall Alert`.

source

Mengidentifikasi layanan yang menghasilkan peristiwa. Untuk acara DNS Firewall, nilai ini adalah `aws.route53resolver`.

detail

Objek JSON yang berisi informasi tentang peristiwa. Layanan yang menghasilkan acara menentukan konten bidang ini.

Untuk acara ini, data ini meliputi:

account-id

ID Akun AWS yang menciptakan VPC.

last-observed-at

Stempel waktu kapan Alert/Block kueri dibuat di VPC.

query-name

Nama domain (example.com) atau nama subdomain (www.example.com) yang ditentukan dalam kueri.

query-type

Entah jenis catatan DNS yang ditentukan dalam permintaan, atau APAPUN. Untuk informasi tentang jenis yang didukung Route 53, lihat [Tipe data DNS yang didukung](#).

query-class

Kelas kueri.

transport

Protokol yang digunakan untuk mengirimkan kueri DNS.

firewall-rule-action

Tindakan yang ditentukan oleh aturan yang cocok dengan nama domain dalam kueri. Baik ALERT atau BLOCK.

firewall-rule-group-id

ID grup aturan Firewall DNS yang cocok dengan nama domain dalam kueri. Untuk informasi selengkapnya tentang grup aturan firewall, lihat DNS Firewall [Grup aturan dan aturan DNS Firewall](#).

firewall-domain-list-id

Daftar domain yang digunakan oleh aturan yang cocok dengan nama domain dalam kueri.

firewall-protection

Perlindungan lanjutan DNS Firewall: DGA, DICTIONARY_DGA, atau DNS_TUNNELING. Untuk informasi selengkapnya, lihat DNS Firewall [Resolver DNS Firewall Lanjutan](#).

resource

Berisi jenis sumber daya dan detail tambahan tentang mereka.

resource-type

Menentukan jenis sumber daya, seperti titik akhir resolver atau contoh VPC.

resource-type-detail

Detail tambahan tentang sumber daya.

Example Acara peringatan DNS Firewall

Berikut ini adalah contoh peristiwa peringatan.

```
{
  "version": "1.0",
  "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
  "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
  "account": "123456789012",
  "time": "2023-05-30T21:52:17Z",
  "region": "us-west-2",
```

```

"resources": [],
"detail": {
  "account-id": "123456789012",
  "last-observed-at": "2023-05-30T20:15:15.900Z",
  "query-name": "15.3.4.32.in-addr.arpa.",
  "query-type": "A",
  "query-class": "IN",
  "transport": "UDP",
  "firewall-rule-action": "ALERT",
  "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
  "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
  "firewall-protection": "DGA",
  "resources": [{
    "resource-type": "instance",
    "instance-details": {
      "id": "i-05746eb48123455e0",
    }
  },
  {
    "resource-type": "resolver-endpoint",
    "resolver-endpoint-details": {
      "id": "i-05746eb48123455e0"
    }
  }
],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
}

```

Detail acara blok DNS Firewall

Di bawah ini adalah bidang detail untuk *event name*.

detail-type Bidang source dan disertakan karena berisi nilai khusus untuk acara Route 53.

```

{...,
  "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
  ...,
  "detail": {
    "account-id": "string",

```

```

    "last-observed-at": "string",
    "query-name": "string",
    "query-type": "string",
    "query-class": "string",
    "transport": "string",
    "firewall-rule-action": "string",
    "firewall-rule-group-id": "string",
    "firewall-domain-list-id": "string",
    "firewall-protection": "string",
    "resources": [{
      "resource-type": "string",
      "instance-details": {
        "id": "string",
      }
    },
    {
      "resource-type": "string",
      "resolver-endpoint-details": {
        "id": "string"
      }
    }
  ]

```

detail-type

Mengidentifikasi jenis acara.

Untuk acara ini, nilai ini adalah `DNS Firewall Alert`.

source

Mengidentifikasi layanan yang menghasilkan peristiwa. Untuk acara DNS Firewall, nilai ini adalah `aws.route53resolver`.

detail

Objek JSON yang berisi informasi tentang peristiwa. Layanan yang menghasilkan acara menentukan konten bidang ini.

Untuk acara ini, data ini meliputi:

account-id

ID Akun AWS yang menciptakan VPC.

`last-observed-at`

Stempel waktu kapan Alert/Block kueri dibuat di VPC.

`query-name`

Nama domain (example.com) atau nama subdomain (www.example.com) yang ditentukan dalam kueri.

`query-type`

Entah jenis catatan DNS yang ditentukan dalam permintaan, atau APAPUN. Untuk informasi tentang jenis yang didukung Route 53, lihat [Tipe data DNS yang didukung](#).

`query-class`

Kelas kueri.

`transport`

Protokol yang digunakan untuk mengirimkan kueri DNS.

`firewall-rule-action`

Tindakan yang ditentukan oleh aturan yang cocok dengan nama domain dalam kueri. Baik ALERT atau BLOCK.

`firewall-rule-group-id`

ID grup aturan Firewall DNS yang cocok dengan nama domain dalam kueri. Untuk informasi selengkapnya tentang grup aturan firewall, lihat DNS Firewall [Grup aturan dan aturan DNS Firewall](#).

`firewall-domain-list-id`

Daftar domain yang digunakan oleh aturan yang cocok dengan nama domain dalam kueri.

`firewall-protection`

Perlindungan lanjutan DNS Firewall: DGA, DICTIONARY_DGA, atau DNS_TUNNELING. Untuk informasi selengkapnya, lihat DNS Firewall [Resolver DNS Firewall Lanjutan](#).

`resource`

Berisi jenis sumber daya dan detail tambahan tentang mereka.

`resource-type`

Menentukan jenis sumber daya, seperti titik akhir resolver atau contoh VPC.

resource-type-detail

Detail tambahan tentang sumber daya.

Example Contoh peristiwa

Berikut ini adalah contoh peristiwa blok.

```
{
  "version": "1.0",
  "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
  "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
  "account": "123456789012",
  "time": "2023-05-30T21:52:17Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "account-id": "123456789012",
    "last-observed-at": "2023-05-30T20:15:15.900Z",
    "query-name": "15.3.4.32.in-addr.arpa.",
    "query-type": "A",
    "query-class": "IN",
    "transport": "UDP",
    "firewall-rule-action": "BLOCK",
    "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
    "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
    "firewall-protection": "DNS_TUNNELING",
    "resources": [{
      "resource-type": "instance",
      "instance-details": {
        "id": "i-05746eb48123455e0"
      }
    },
    {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
        "id": "i-05746eb48123455e0",
      }
    }
  ],
  "src-addr": "4.5.64.102",
  "src-port": "56067",
```

```
"vpc-id": "vpc-7example"  
}  
}
```

Mencatat panggilan API Amazon Route 53 dengan AWS CloudTrail

Route 53 terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Route 53. CloudTrail menangkap semua panggilan API untuk Route 53 sebagai peristiwa, termasuk panggilan dari konsol Route 53 dan dari panggilan kode ke Route 53 APIs. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Route 53. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Route 53, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Topik

- [Informasi rute 53 di CloudTrail](#)
- [Melihat peristiwa Route 53 dalam riwayat peristiwa](#)
- [Memahami entri berkas log Route 53](#)

Informasi rute 53 di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Rute 53, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Route 53, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol, jejak ini diterapkan ke semua Wilayah. Trail mencatat peristiwa dari semua wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi lebih lanjut, lihat:

- [Ikhtisar untuk membuat jejak](#)

- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa Wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Semua tindakan Route 53 dicatat oleh CloudTrail dan didokumentasikan dalam [Referensi API Amazon Route 53](#). Misalnya, panggilan ke `CreateHostedZone`, `CreateHealthCheck`, dan `RegisterDomain` tindakan menghasilkan entri dalam file CloudTrail log.

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

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

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Melihat peristiwa Route 53 dalam riwayat peristiwa

CloudTrail memungkinkan Anda melihat peristiwa terbaru dalam riwayat Acara. Untuk melihat peristiwa untuk permintaan API Route 53, Anda harus memilih US East (N. Virginia) pada pemilih wilayah di bagian atas konsol. Untuk informasi selengkapnya, lihat [Melihat CloudTrail peristiwa dengan riwayat peristiwa](#) di Panduan AWS CloudTrail Pengguna.

Memahami entri berkas log Route 53

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

Elemen `eventName` mengidentifikasi tindakan yang terjadi. (Dalam CloudTrail log, huruf pertama adalah huruf kecil untuk tindakan pendaftaran domain meskipun huruf besar dalam nama tindakan.

Misalnya, UpdateDomainContact muncul seperti updateDomainContact di log). CloudTrail mendukung semua tindakan API Route 53. Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan tindakan berikut:

- Buat daftar zona yang dihosting yang terkait dengan AWS akun
- Membuat pemeriksaan kondisi
- Membuat dua catatan
- Menghapus zona yang di-hosting
- Memperbarui informasi untuk domain terdaftar
- Buat titik akhir keluar Route 53 VPC Resolver

```
{
  "Records": [
    {
      "apiVersion": "2013-04-01",
      "awsRegion": "us-east-1",
      "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
      "eventName": "ListHostedZones",
      "eventSource": "route53.amazonaws.com",
      "eventTime": "2015-01-16T00:41:48Z",
      "eventType": "AwsApiCall",
      "eventVersion": "1.02",
      "recipientAccountId": "444455556666",
      "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
      "requestParameters": null,
      "responseElements": null,
      "sourceIPAddress": "192.0.2.92",
      "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
      "userIdentity": {
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "type": "IAMUser",
        "userName": "smithj"
      }
    },
    {
      "apiVersion": "2013-04-01",
      "awsRegion": "us-east-1",
```

```

    "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
    "eventName": "CreateHealthCheck",
    "eventSource": "route53.amazonaws.com",
    "eventTime": "2018-01-16T00:41:57Z",
    "eventType": "AwsApiCall",
    "eventVersion": "1.02",
    "recipientAccountId": "444455556666",
    "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
    "requestParameters": {
      "callerReference": "2014-05-06 64832",
      "healthCheckConfig": {
        "ipAddress": "192.0.2.249",
        "port": 80,
        "type": "TCP"
      }
    },
    "responseElements": {
      "healthCheck": {
        "callerReference": "2014-05-06 64847",
        "healthCheckConfig": {
          "failureThreshold": 3,
          "ipAddress": "192.0.2.249",
          "port": 80,
          "requestInterval": 30,
          "type": "TCP"
        },
        "healthCheckVersion": 1,
        "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
      },
      "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
    },
    "sourceIPAddress": "192.0.2.92",
    "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
    "userIdentity": {
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "accountId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "type": "IAMUser",
      "userName": "smithj"
    }
  },
  {

```

```
"additionalEventData": {
  "Note": "Do not use to reconstruct hosted zone"
},
"apiVersion": "2013-04-01",
"awsRegion": "us-east-1",
"eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
"eventName": "ChangeResourceRecordSets",
"eventSource": "route53.amazonaws.com",
"eventTime": "2018-01-16T00:41:43Z",
"eventType": "AwsApiCall",
"eventVersion": "1.02",
"recipientAccountId": "444455556666",
"requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
"requestParameters": {
  "changeBatch": {
    "changes": [
      {
        "action": "CREATE",
        "resourceRecordSet": {
          "name": "prod.example.com.",
          "resourceRecords": [
            {
              "value": "192.0.1.1"
            },
            {
              "value": "192.0.1.2"
            },
            {
              "value": "192.0.1.3"
            },
            {
              "value": "192.0.1.4"
            }
          ],
          "ttl": 300,
          "type": "A"
        }
      },
      {
        "action": "CREATE",
        "resourceRecordSet": {
          "name": "test.example.com.",
          "resourceRecords": [
            {
```

```

        "value": "192.0.1.1"
      },
      {
        "value": "192.0.1.2"
      },
      {
        "value": "192.0.1.3"
      },
      {
        "value": "192.0.1.4"
      }
    ],
    "ttl": 300,
    "type": "A"
  }
},
"comment": "Adding subdomains"
},
"hostedZoneId": "Z1PA6795UKMFR9"
},
"responseElements": {
  "changeInfo": {
    "comment": "Adding subdomains",
    "id": "/change/C156SRE0X2ZB10",
    "status": "PENDING",
    "submittedAt": "Jan 16, 2018 12:41:43 AM"
  }
},
"sourceIPAddress": "192.0.2.92",
"userAgent": "Apache-HttpClient/4.3 (java 1.5)",
"userIdentity": {
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "accountId": "111122223333",
  "arn": "arn:aws:iam::111122223333:user/smithj",
  "principalId": "A1B2C3D4E5F6G7EXAMPLE",
  "type": "IAMUser",
  "userName": "smithj"
}
},
{
  "apiVersion": "2013-04-01",
  "awsRegion": "us-east-1",
  "eventID": "0cb87544-ebce-40a9-9812-e9dda1962cb2",

```

```

    "eventName": "DeleteHostedZone",
    "eventSource": "route53.amazonaws.com",
    "eventTime": "2018-01-16T00:41:37Z",
    "eventType": "AwsApiCall",
    "eventVersion": "1.02",
    "recipientAccountId": "444455556666",
    "requestID": "6d5d149f-9d18-11e4-b752-f9c6311f3510",
    "requestParameters": {
      "id": "Z1PA6795UKMFR9"
    },
    "responseElements": {
      "changeInfo": {
        "id": "/change/C1SIJYUYIKVJWP",
        "status": "PENDING",
        "submittedAt": "Jan 16, 2018 12:41:36 AM"
      }
    },
    "sourceIPAddress": "192.0.2.92",
    "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
    "userIdentity": {
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "accountId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "type": "IAMUser",
      "userName": "smithj"
    }
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "smithj",
      "sessionContext": {
        "attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2018-11-01T19:43:59Z"
        }
      }
    },
    "invokedBy": "test"
  }
}

```



```

    },
    "eventTime": "2018-11-01T19:49:36Z",
    "eventSource": "route53domains.amazonaws.com",
    "eventName": "updateDomainContact",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.92",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
    "requestParameters": {
        "domainName": {
            "name": "example.com"
        }
    },
    "responseElements": {
        "requestId": "034e222b-a3d5-4bec-8ff9-35877ff02187"
    },
    "additionalEventData": "Personally-identifying contact information is not
logged in the request",
    "requestID": "015b7313-bf3d-11e7-af12-cf75409087f6",
    "eventID": "f34f3338-aaf4-446f-bf0e-f72323bac94d",
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-01T14:33:09Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIUZEZLWWZOEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            }
        }
    }
}

```

```

    },
    "eventTime": "2018-11-01T14:37:19Z",
    "eventSource": "route53resolver.amazonaws.com",
    "eventName": "CreateResolverEndpoint",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
    "requestParameters": {
        "creatorRequestId": "123456789012",
        "name": "OutboundEndpointDemo",
        "securityGroupIds": [
            "sg-05618b249example"
        ],
        "direction": "OUTBOUND",
        "ipAddresses": [
            {
                "subnetId": "subnet-01cb0c4676example"
            },
            {
                "subnetId": "subnet-0534819b32example"
            }
        ],
        "tags": []
    },
    "responseElements": {
        "resolverEndpoint": {
            "id": "rslvr-out-1f4031f1f5example",
            "creatorRequestId": "123456789012",
            "arn": "arn:aws:route53resolver:us-west-2:123456789012:resolver-
endpoint/rslvr-out-1f4031f1f5example",
            "name": "OutboundEndpointDemo",
            "securityGroupIds": [
                "sg-05618b249example"
            ],
            "direction": "OUTBOUND",
            "ipAddressCount": 2,
            "hostVPCId": "vpc-0de29124example",
            "status": "CREATING",
            "statusMessage": "[Trace id: 1-5bd1d51e-f2f3032eb75649f71example]
Creating the Resolver Endpoint",
            "creationTime": "2018-11-01T14:37:19.045Z",
            "modificationTime": "2018-11-01T14:37:19.045Z"
        }
    }
}

```

```
    },  
    "requestID": "3f066d98-773f-4628-9cba-4ba6eexample",  
    "eventID": "cb05b4f9-9411-4507-813b-33cb0example",  
    "eventType": "AwsApiCall",  
    "recipientAccountId": "123456789012"  
  }  
]  
}
```

Pemecahan masalah Amazon Route 53

Halaman ini mencakup topik pemecahan masalah berikut untuk Amazon Route 53:

1. Ketidaktersediaan domain:

- Pahami alasan umum mengapa domain Anda mungkin tidak tersedia di internet, seperti tidak mengonfirmasi email pendaftar, masalah transfer layanan DNS, pengaturan server nama yang salah, atau zona host yang dihapus.

2. Penangguhan domain:

- Pelajari tentang penyebab penangguhan domain (ClientHold status) dan cara agar domain Anda tidak ditangguhkan, termasuk domain kedaluwarsa, perubahan email pendaftar yang tidak diverifikasi, dan masalah pemrosesan pembayaran.

3. Operasi domain yang gagal:

- Mengatasi kegagalan operasi domain termasuk pendaftaran, transfer, perpanjangan, dan masalah pembaruan kontak yang disebabkan oleh informasi kontak yang tidak valid.

4. Transfer domain gagal:

- Temukan alasan umum untuk transfer domain gagal ke Route 53, seperti tidak mengotorisasi transfer, kode otorisasi yang tidak valid, atau masalah dengan nama domain internasional.

5. Pengaturan DNS tidak berlaku:

- Memecahkan masalah di mana perubahan pengaturan DNS Anda belum berlaku, termasuk cache penyelesai DNS, pembaruan server nama yang salah, dan beberapa zona yang dihosting dengan nama yang sama.

6. Kesalahan “Server Tidak Ditemukan”:

- Temukan solusi untuk kesalahan “Server Tidak Ditemukan” di browser Anda, seperti catatan yang hilang, nilai catatan yang salah, atau sumber daya yang tidak tersedia.

7. Merutekan lalu lintas ke bucket S3:

- Selesaikan masalah saat mencoba merutekan lalu lintas ke bucket Amazon S3 yang dikonfigurasi untuk hosting situs web.

8. Masalah penagihan:

- Pahami skenario penagihan umum, termasuk ditagih dua kali untuk zona host yang sama, beberapa faktur untuk domain, dan masalah pendaftaran domain saat Anda ditutup atau ditutup Akun AWS secara permanen.

Topik

- [Domain saya tidak tersedia di internet](#)
- [Domain saya ditangguhkan \(statusnya ClientHold\)](#)
- [Operasi domain saya gagal](#)
- [Gagal mentransfer domain saya ke Amazon Route 53](#)
- [Saya mengubah pengaturan DNS, tetapi mereka belum diterapkan](#)
- [Peramban saya menampilkan kesalahan "Server tidak ditemukan"](#)
- [Saya tidak dapat merutekan lalu lintas ke bucket Amazon S3 yang dikonfigurasi untuk meng-host situs web](#)
- [Saya ditagih dua kali untuk zona yang di-hosting yang sama](#)
- [Saya ditagih beberapa faktur untuk domain saya](#)
- [AWS Akun saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53](#)

Domain saya tidak tersedia di internet

Berikut adalah alasan paling umum bahwa domain Anda tidak tersedia di internet.

Topik

- [Anda mendaftarkan domain baru, tetapi tidak mengeklik tautan di email konfirmasi](#)
- [Anda mentransfer pendaftaran domain ke Amazon Route 53, tetapi Anda tidak mentransfer layanan DNS](#)
- [Anda ditransfer pendaftaran domain dan menentukan server nama yang salah dalam pengaturan domain](#)
- [Anda mentransfer layanan DNS terlebih dahulu, tetapi Anda tidak menunggu cukup lama sebelum mentransfer pendaftaran domain](#)
- [Anda menghapus zona host yang digunakan Route 53 untuk merutekan lalu lintas internet untuk domain](#)
- [Domain Anda telah ditangguhkan](#)

Anda mendaftarkan domain baru, tetapi tidak mengeklik tautan di email konfirmasi

Saat Anda mendaftarkan domain baru, ICANN mengharuskan kami mendapatkan konfirmasi bahwa alamat email untuk kontak pendaftar valid. Untuk mendapatkan konfirmasi, kami mengirim email yang berisi tautan. (Jika Anda tidak menanggapi email pertama, kami mengirim ulang email yang sama hingga dua kali.) Anda memiliki waktu antara 3 dan 15 hari untuk mengeklik tautan, tergantung domain tingkat atas. Setelah waktu itu, tautan berhenti bekerja.

Jika Anda tidak mengeklik tautan di email dalam jumlah waktu yang ditentukan, ICANN mengharuskan kami menanggapi domain tersebut. Untuk informasi tentang cara mengirim ulang email konfirmasi ke kontak pendaftar, lihat [Mengirim ulang email otorisasi dan konfirmasi](#).

Anda mentransfer pendaftaran domain ke Amazon Route 53, tetapi Anda tidak mentransfer layanan DNS

Jika registrar sebelumnya menawarkan layanan DNS gratis dengan pendaftaran domain, registrar mungkin berhenti menyediakan layanan DNS saat Anda mentransfer pendaftaran domain ke Route 53. Lakukan prosedur berikut untuk menentukan apakah ini adalah masalah dan, jika demikian, cara untuk mengatasinya.

Untuk memulihkan layanan DNS jika registrar sebelumnya membatalkannya setelah Anda mentransfer pendaftaran domain ke Route 53

1. Hubungi registrar sebelumnya dan konfirmasikan bahwa mereka membatalkan layanan DNS untuk domain Anda. Jika demikian, berikut adalah tiga cara tercepat untuk memulihkan layanan DNS untuk domain, dalam urutan keinginan:
 - Jika registrar sebelumnya menyediakan layanan DNS berbayar, mintalah mereka untuk memulihkan layanan DNS menggunakan data DNS lama dan server nama untuk domain Anda.
 - Jika registrar sebelumnya tidak menyediakan layanan DNS berbayar tanpa registrasi domain, tanyakan apakah Anda dapat mentransfer kembali pendaftaran domain dan meminta mereka memulihkan layanan DNS menggunakan data DNS lama dan server nama untuk domain Anda.
 - Jika Anda dapat mentransfer pendaftaran domain kembali ke registrar sebelumnya tetapi mereka tidak memiliki catatan DNS Anda lagi, tanyakan apakah Anda dapat mentransfer kembali pendaftaran domain ke registrar tersebut dan mendapatkan rangkaian nama server

yang sama yang sebelumnya ditetapkan ke domain tersebut. Jika hal ini memungkinkan, Anda harus membuat ulang data DNS lama Anda sendiri. Namun, segera setelah Anda melakukannya, domain Anda akan tersedia lagi.

Jika registrar sebelumnya tidak dapat membantu dengan salah satu opsi ini, lanjutkan dengan langkah 2.

 Important

Jika Anda tidak dapat memulihkan layanan DNS menggunakan server nama yang Anda tentukan saat mentransfer domain ke Route 53, diperlukan waktu hingga dua hari setelah Anda menyelesaikan langkah-langkah yang tersisa dalam prosedur ini agar domain Anda tersedia lagi di internet. DNS resolver biasanya men-cache nama server nama untuk domain selama 24 hingga 48 jam, dan itu akan memakan waktu lama sebelum semua DNS resolver mendapatkan nama server nama baru.

2. Pilih layanan DNS baru, misalnya, Route 53.
3. Menggunakan metode yang disediakan oleh layanan DNS baru, membuat zona yang di-hosting dan catatan:
 - a. Buat zona yang di-hosting yang memiliki nama yang sama dengan domain Anda, misalnya example.com.
 - b. Gunakan file zona yang Anda dapatkan dari registrar sebelumnya untuk membuat catatan.

Jika Anda memilih Route 53 sebagai layanan DNS baru, Anda dapat membuat catatan dengan mengimpor file zona. Untuk informasi selengkapnya, lihat [Membuat catatan dengan mengimpor file zona](#).

4. Dapatkan server nama untuk zona yang di-hosting baru. Jika Anda memilih Route 53 sebagai layanan DNS, lihat [Mendapatkan server nama untuk zona yang di-hosting publik](#).
5. Ubah server nama untuk domain Anda ke server nama yang Anda dapatkan di langkah 4. Untuk informasi selengkapnya, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).

Anda ditransfer pendaftaran domain dan menentukan server nama yang salah dalam pengaturan domain

Saat Anda mentransfer pendaftaran domain ke Amazon Route 53, salah satu pengaturan yang Anda tentukan untuk domain adalah kumpulan server nama yang akan merespons kueri DNS untuk domain tersebut. Server nama ini berasal dari zona yang di-hosting yang memiliki nama yang sama sebagai domain. Zona yang di-hosting berisi informasi tentang bagaimana Anda ingin rute lalu lintas untuk domain, seperti alamat IP dari server web untuk `www.example.com`.

Anda mungkin telah sengaja menentukan nama server untuk zona yang di-hosting yang salah, yang sangat mudah jika Anda memiliki lebih dari satu zona yang di-hosting yang memiliki nama yang sama dengan domain. Untuk mengonfirmasi bahwa domain menggunakan server nama untuk zona yang di-hosting yang benar dan, jika perlu, memperbarui server nama untuk domain, lakukan prosedur berikut.

Important

Jika Anda menetapkan data server nama yang salah ketika Anda mentransfer domain ke Route 53, itu dapat memakan waktu hingga dua hari setelah Anda memperbaiki server nama untuk domain sebelum layanan DNS sepenuhnya dipulihkan. Ini karena DNS resolver di internet biasanya meminta server nama hanya sekali setiap dua hari dan menyimpan jawabannya.

Untuk mendapatkan server nama untuk zona yang di-hosting

1. Jika Anda menggunakan layanan DNS lain untuk domain, menggunakan metode yang disediakan oleh layanan DNS untuk mendapatkan server nama zona yang di-hosting. Kemudian, lewati ke prosedur berikutnya.

Jika Anda menggunakan Route 53 sebagai layanan DNS untuk domain, masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

2. Pada panel navigasi, pilih Hosted Zones (Zona yang di-hosting).
3. Pada halaman Hosted Zones (Zona yang di-hosting), pilih tombol radio (bukan nama) untuk zona yang di-hosting.

 Important

Jika Anda memiliki lebih dari satu zona yang di-hosting dengan nama yang sama, pastikan Anda mendapatkan server nama untuk zona yang di-hosting yang benar.

4. Di panel kanan, buat catatan dari empat server terdaftar untuk Server.

Untuk mengonfirmasi bahwa domain menggunakan server nama yang benar

1. Jika Anda menggunakan layanan DNS lain untuk domain, masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>

Jika Anda menggunakan Route 53, lewati ke langkah berikutnya.

2. Di panel navigasi, pilih Registered Domains (Domain terdaftar).
3. Pilih nama domain yang ingin Anda edit pengaturannya.
4. Pilih Add or Edit Name Servers (Tambah atau Edit Server Nama).
5. Bandingkan daftar server nama yang Anda dapatkan di prosedur sebelumnya dengan server nama yang tercantum di kotak dialog Edit Name Servers for (Edit Nama Server untuk) domain name(nama domain).
6. Jika server nama yang tercantum di sini tidak cocok dengan server nama yang Anda dapatkan di prosedur sebelumnya, ubah server nama di sini, lalu pilih Update (Perbarui).

Anda mentransfer layanan DNS terlebih dahulu, tetapi Anda tidak menunggu cukup lama sebelum mentransfer pendaftaran domain

Ketika Anda mentransfer layanan DNS ke Amazon Route 53 atau layanan DNS lainnya, Anda memperbarui konfigurasi untuk domain Anda dengan registrar domain untuk menggunakan server nama untuk layanan DNS baru.

DNS resolver, yang menanggapi permintaan untuk domain Anda, biasanya menyimpan nama server nama selama 24 hingga 48 jam. Jika Anda mengubah layanan DNS untuk domain dan mengganti server nama dari satu layanan DNS dengan server nama untuk layanan DNS lain, ini dapat memakan waktu hingga 48 jam sebelum DNS resolver mulai menggunakan server nama baru dan, oleh karena itu, terdapat layanan DNS baru.

Inilah cara mentransfer layanan DNS Anda dan kemudian mentransfer domain Anda terlalu cepat setelah itu dapat menyebabkan domain Anda menjadi tidak tersedia di internet:

1. Anda mentransfer layanan DNS untuk domain Anda.
2. Anda mentransfer domain Anda ke Route 53 sebelum DNS resolver mulai menggunakan server nama untuk layanan DNS baru Anda.
3. Registrar Anda sebelumnya membatalkan layanan DNS untuk domain Anda segera setelah domain dipindahkan ke Route 53.
4. DNS resolver masih merutekan kueri ke layanan DNS lama Anda, tetapi tidak ada lagi catatan yang menjelaskan cara merutekan lalu lintas Anda.

Saat cache kedaluwarsa untuk server nama untuk layanan DNS lama, DNS akan mulai menggunakan layanan DNS baru Anda. Sayangnya, tidak ada cara untuk mempercepat proses ini.

Anda menghapus zona host yang digunakan Route 53 untuk merutekan lalu lintas internet untuk domain

Jika Route 53 adalah layanan DNS untuk domain Anda dan jika Anda menghapus zona host yang digunakan untuk merutekan lalu lintas internet untuk domain, domain akan menjadi tidak tersedia di internet. Hal ini berlaku terlepas dari apakah domain terdaftar dengan Route 53.

Important

Mengembalikan layanan internet untuk domain dapat memakan waktu hingga 48 jam.

Untuk memulihkan layanan internet jika Anda menghapus zona host yang digunakan Route 53 untuk merutekan lalu lintas internet untuk domain

1. Membuat zona yang di-hosting lain yang memiliki nama yang sama dengan domain. Untuk informasi selengkapnya, lihat [Membuat zona yang di-hosting publik](#).
2. Membuat ulang catatan yang berada di zona yang di-hosting yang Anda dihapus. Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).
3. Dapatkan nama server nama yang ditetapkan Route 53 ke zona yang di-hosting yang baru. Untuk informasi selengkapnya, lihat [Mendapatkan server nama untuk zona yang di-hosting publik](#).

4. Memperbarui pendaftaran domain untuk menggunakan server nama yang Anda dapatkan di langkah 3:
 - Jika domain terdaftar dengan Route 53, lihat [Menambahkan atau mengubah server nama dan merekatkan catatan untuk domain](#).
 - Jika domain terdaftar dengan registrar domain lain, gunakan metode yang disediakan oleh registrar untuk memperbarui pendaftaran domain agar menggunakan server nama baru.
5. Tunggu TTL hingga server nama melewati resolver rekursif yang telah menyimpan nama server nama untuk zona yang di-hosting yang dihapus dalam cache. Setelah TTL telah berlalu, ketika peramban atau aplikasi mengirimkan permintaan DNS untuk domain atau salah satu subdomain, resolver rekursif meneruskan permintaan ke server nama Route 53 untuk zona yang di-hosting baru. Untuk informasi selengkapnya, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

TTL untuk server nama dapat selama 48 jam, tergantung TLD domain.

Domain Anda telah ditangguhkan

Domain Anda mungkin tidak tersedia di internet karena kami harus menangguhkannya. Untuk informasi selengkapnya, lihat [Domain saya ditangguhkan \(statusnya ClientHold\)](#).

Domain saya ditangguhkan (statusnya ClientHold)

Jika Amazon Route 53 menunda domain Anda, domain menjadi tidak tersedia di internet. Anda dapat menggunakan salah satu metode berikut untuk menentukan apakah domain telah ditangguhkan:

- Pada halaman Domain terdaftar konsol Route 53, menemukan nama domain di tabel Peringatan di bagian bawah halaman. Jika nilai dari kolom Status adalah `clientHold`, domain telah ditangguhkan.
- Kirim kueri WHOIS untuk domain tersebut. Jika nilai dari Status Domain adalah `clientHold`, domain telah ditangguhkan. Perintah WHOIS tersedia di banyak sistem operasi, dan juga tersedia sebagai aplikasi web di banyak situs web.

Selain itu, saat kami menangguhkan domain, kami biasanya mengirim email ke alamat email untuk kontak pendaftar untuk domain tersebut. Namun, jika domain ditangguhkan berdasarkan perintah pengadilan, pengadilan mungkin tidak mengizinkan kami memberi tahu kontak pendaftar.

Untuk membuat domain tersedia lagi di internet, Anda harus membatalkan penangguhannya. Berikut adalah alasan domain dapat ditangguhkan dan bagaimana Anda membatalkan penangguhannya.

 Note

Jika Anda memerlukan bantuan agar domain Anda tidak ditangguhkan, Anda dapat menghubungi AWS Support secara gratis. Untuk informasi selengkapnya, lihat [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Topik

- [Anda mendaftarkan domain baru, tetapi tidak mengeklik tautan di email konfirmasi](#)
- [Anda menonaktifkan perpanjangan otomatis untuk domain, dan domain kedaluwarsa](#)
- [Anda mengubah alamat email untuk kontak pendaftar, tetapi Anda tidak memverifikasi bahwa alamat email baru itu valid](#)
- [Kami tidak dapat memproses pembayaran Anda untuk perpanjangan domain otomatis, dan domain kedaluwarsa](#)
- [Kami menangguhkan domain untuk pelanggaran Kebijakan Penggunaan yang Diterima AWS](#)
- [Kami menangguhkan domain karena perintah pengadilan](#)

Anda mendaftarkan domain baru, tetapi tidak mengeklik tautan di email konfirmasi

Saat Anda mendaftarkan domain AWS untuk pertama kalinya, ICANN mengharuskan kami mendapatkan konfirmasi bahwa alamat email untuk kontak pendaftar valid. Untuk mendapatkan konfirmasi, kami mengirim email yang berisi tautan. Anda memiliki waktu antara 3 dan 15 hari untuk mengeklik tautan, tergantung domain tingkat atas. Setelah waktu itu, tautan berhenti bekerja.

 Note

Jika Anda telah mendaftarkan satu atau beberapa domain dengan Amazon Route 53 dan menggunakan alamat email yang sama untuk kontak pendaftar, kami tidak akan mengirimkan email konfirmasi.

Jika Anda tidak mengeklik tautan di email dalam jumlah waktu yang ditentukan, ICANN mengharuskan kami menangguhkan domain tersebut. Untuk informasi tentang cara mengirim ulang email konfirmasi ke kontak pendaftar, lihat [Mengirim ulang email otorisasi dan konfirmasi](#). Bila Anda mengonfirmasi bahwa alamat email valid, kami secara otomatis membatalkan penangguhan domain tersebut.

Anda menonaktifkan perpanjangan otomatis untuk domain, dan domain kedaluwarsa

Ketika perpanjangan otomatis diaktifkan untuk domain (nilai default untuk domain baru atau yang ditransfer), kami secara otomatis memperbarui pendaftaran untuk domain tersebut sesaat sebelum tanggal kedaluwarsa. Jika Anda menonaktifkan perpanjangan otomatis, kami akan mengirimkan tiga email pengingat bahwa pendaftaran domain akan kedaluwarsa ke alamat email kontak pendaftar. Kami mulai mengirim email ini 45 hari sebelum domain kedaluwarsa.

Jika Anda menonaktifkan perpanjangan otomatis untuk domain tersebut dan Anda tidak memperpanjang masa pendaftaran domain secara manual, biasanya kami menangguhkan domain tersebut pada tanggal kedaluwarsa. Perhatikan bahwa pendaftar untuk beberapa domain menghapus domain bahkan sebelum tanggal kedaluwarsa.

Untuk informasi tentang cara memperbarui domain kedaluwarsa, lihat [Memperbarui pendaftaran untuk domain](#).

Anda mengubah alamat email untuk kontak pendaftar, tetapi Anda tidak memverifikasi bahwa alamat email baru itu valid

Jika Anda mengubah alamat email untuk kontak pendaftar ke alamat yang belum Anda verifikasi sebelumnya, ICANN mengharuskan kami mendapatkan konfirmasi bahwa alamat email untuk kontak pendaftar valid. Untuk mendapatkan konfirmasi, kami mengirim email yang berisi tautan. Anda memiliki waktu antara 3 dan 15 hari untuk mengeklik tautan, tergantung domain tingkat atas. Setelah waktu itu, tautan berhenti bekerja.

Jika Anda tidak mengeklik tautan dalam email dalam jumlah waktu yang diizinkan oleh registri TLD, ICANN mengharuskan kami menangguhkan domain tersebut. Untuk informasi tentang cara mengirim ulang email konfirmasi ke kontak pendaftar, lihat [Mengirim ulang email otorisasi dan konfirmasi](#). Bila Anda mengonfirmasi bahwa alamat email valid, kami secara otomatis membatalkan penangguhan domain tersebut.

Kami tidak dapat memproses pembayaran Anda untuk perpanjangan domain otomatis, dan domain kedaluwarsa

Jika perpanjangan otomatis diaktifkan untuk domain tetapi kami tidak dapat memproses pembayaran Anda (misalnya, karena kartu kredit Anda kedaluwarsa), kami mengirim beberapa email ke alamat email untuk kontak pendaftar untuk domain tersebut. Jika kami tidak menerima pembayaran, kami biasanya menangguhkan domain pada tanggal kedaluwarsa. Perhatikan bahwa pendaftar untuk beberapa domain menghapus domain bahkan sebelum tanggal kedaluwarsa.

Untuk informasi tentang cara memperbarui domain kedaluwarsa, lihat [Memperbarui pendaftaran untuk domain](#).

Kami menangguhkan domain untuk pelanggaran Kebijakan Penggunaan yang Diterima AWS

Jika kami menangguhkan domain untuk pelanggaran [Kebijakan Penggunaan yang Diterima AWS](#), kami akan mengirimkan pemberitahuan email ke kontak pendaftar untuk domain tersebut. (Kami tidak mengirim email pemberitahuan jika AWS akun sudah ditangguhkan karena penipuan.)

Untuk menentang penangguhan, kirim email ke trustandsafety@support.aws.com.

Kami menangguhkan domain karena perintah pengadilan

Jika domain ditangguhkan sebagai akibat dari perintah pengadilan, kami tidak dapat menghentikan penangguhan domain sampai perintah pengadilan telah dicabut. Untuk menentang validitas perintah pengadilan, kirim email ke trustandsafety@support.aws.com dan lampirkan dokumen yang berlaku.

Operasi domain saya gagal

Berikut adalah beberapa tips pemecahan masalah jika operasi domain Anda gagal. Operasi dapat berupa pendaftaran, transfer, pembaruan, atau pembaruan kontak.

Operasi domain gagal karena informasi kontak yang tidak valid

Jika operasi domain gagal dengan kesalahan tentang informasi kontak yang tidak valid, detail kontak yang Anda berikan tidak memenuhi persyaratan validasi registri.

Untuk mengatasi masalah ini, verifikasi bahwa semua detail kontak diformat dengan benar:

- Nama - Pastikan nama hanya berisi karakter yang valid dan diformat dengan benar.
- Alamat — Konfirmasikan bahwa format alamat sesuai dengan standar pos untuk negara tersebut.
- Nomor telepon — Gunakan format internasional yang benar untuk negara tersebut.
- Bidang identifikasi — Untuk domain yang memerlukan nomor identifikasi, pastikan formatnya benar untuk negara yang ditentukan.

Setelah Anda memperbaiki informasi kontak, coba operasi domain lagi. Untuk persyaratan khusus untuk domain tingkat atas yang berbeda, lihat. [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#)

Gagal mentransfer domain saya ke Amazon Route 53

Jika transfer domain Anda telah gagal atau ditolak, gunakan bagian ini untuk mendiagnosis dan menyelesaikan kegagalan.

Note

Untuk mencegah masalah selama transfer aktif, lihat [Mencegah masalah transfer Route 53 yang umum](#).

Topik

- [Anda tidak mengeklik tautan di email otorisasi](#)
- [Kode otorisasi yang Anda dapatkan dari registrar saat ini tidak valid](#)
- [Kesalahan "Parameter dalam permintaan tidak valid" saat mencoba mentransfer domain .es ke Amazon Route 53](#)
- [Apakah nama domain internasional yang Anda transfer ke Amazon Route 53 terdaftar di punycode?](#)
- [Pesan kesalahan transfer umum](#)

Anda tidak mengeklik tautan di email otorisasi

Saat Anda mentransfer pendaftaran domain ke Amazon Route 53, kami diwajibkan oleh ICANN, badan pengelola untuk pendaftaran domain, untuk mendapatkan otorisasi transfer dari kontak pendaftar untuk domain tersebut. Untuk mendapatkan otorisasi, kami mengirimkan email yang berisi

tautan. Anda memiliki waktu antara 5 dan 15 hari untuk mengeklik tautan, tergantung pada domain tingkat atas. Setelah waktu itu, tautan berhenti bekerja.

Jika Anda tidak mengeklik tautan dalam email dalam jumlah waktu yang ditentukan, ICANN mengharuskan kami membatalkan transfer. Untuk selengkapnya tentang cara mengirim ulang email otorisasi ke kontak pendaftar, lihat [Mengirim ulang email otorisasi dan konfirmasi](#).

Kode otorisasi yang Anda dapatkan dari registrar saat ini tidak valid

Jika Anda meminta transfer domain ke Amazon Route 53 dan Anda tidak menerima email otorisasi, lihat [halaman status di konsol Route 53](#). Jika halaman status menunjukkan bahwa kode otorisasi transfer yang Anda dapatkan dari registrar tidak valid, lakukan langkah-langkah berikut:

1. Hubungi registrar saat ini untuk domain dan minta kode otorisasi baru. Konfirmasi hal berikut:
 - Berapa lama kode otorisasi baru akan tetap aktif. Anda harus meminta transfer domain sebelum kode kedaluwarsa.
 - Kode otorisasi baru berbeda dari kode yang tidak valid. Jika tidak, mintalah registrar saat ini untuk menyegarkan kode otorisasi.
2. Kirim permintaan lain untuk mentransfer domain. Untuk informasi selengkapnya, lihat [Langkah 5: Minta transfer](#) dalam topik [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#).

Kesalahan "Parameter dalam permintaan tidak valid" saat mencoba mentransfer domain .es ke Amazon Route 53

Amazon Route 53 mengembalikan kesalahan "Parameter dalam permintaan tidak valid" saat Anda mencoba mentransfer domain .es ke Route 53 dan jenis kontak dari kontak pendaftar adalah Perusahaan. Untuk menyelesaikan transfer, ubah jenis kontak pendaftar menjadi Orang, dan kirim kembali.

Apakah nama domain internasional yang Anda transfer ke Amazon Route 53 terdaftar di punycode?

Ketika mendaftarkan nama domain baru atau membuat zona yang di-hosting dan catatan, Anda dapat menentukan huruf selain a-z (misalnya, ç dalam bahasa Prancis), karakter dalam huruf lain (misalnya, Sirilik atau Arab), dan karakter dalam bahasa Cina, Jepang, atau Korea. Amazon Route 53 menyimpan nama domain internasional ini (IDNs) di Punycode, yang mewakili karakter Unicode sebagai string ASCII.

Jika Anda mendapatkan kesalahan saat mentransfer IDNs ke Route 53, gunakan punycode untuk mewakilinya dan coba lagi. Untuk informasi selengkapnya, lihat [Memformat nama domain yang diinternasionalisasi](#).

Pesan kesalahan transfer umum

Ketika transfer domain gagal, Anda biasanya akan menerima pesan kesalahan baik di konsol Route 53 atau melalui email. Berikut adalah pesan kesalahan yang paling umum dan cara mengatasinya:

“Transfer ditolak oleh registri”

Kesalahan ini terjadi ketika registri domain memblokir transfer karena salah satu dari beberapa alasan. Penyebab paling umum adalah:

- Domain tidak memenuhi aturan ICANN 60 hari. ICANN mengharuskan transfer diblokir dalam waktu 60 hari sejak pendaftaran awal atau perubahan kontak pendaftar.
- Domain telah mengaktifkan kunci transfer di registrar Anda saat ini.
- Domain berada dalam status yang mencegah transfer, seperti `clientTransferProhibited`, `serverTransferProhibited`, `pendingDelete`, `pendingTransfer`, atau `redemptionPeriod`.

Untuk mengatasi masalah ini, periksa hal berikut dengan registrar Anda saat ini:

- Verifikasi bahwa domain tersebut berusia lebih dari 60 hari sejak tanggal pendaftaran. Jika Anda baru saja mengubah informasi kontak pendaftar, Anda mungkin perlu menunggu 60 hari sejak perubahan itu. Beberapa pendaftar mengizinkan Anda untuk memilih keluar dari pembatasan ini, jadi tanyakan kepada pencatat Anda saat ini apakah opsi ini tersedia.
- Buka kunci domain dengan menonaktifkan kunci transfer atau kunci domain apa pun.
- Periksa apakah status domain Anda memungkinkan transfer. Anda dapat memverifikasi status domain menggunakan pencarian WHOIS atau dengan menghubungi registrar Anda saat ini.

“Kode otorisasi tidak valid” atau “Kode autentikasi salah”

Kesalahan ini berarti bahwa kode otorisasi (juga disebut kode EPP atau kode transfer) yang Anda masukkan tidak valid. Hal ini dapat terjadi jika kode telah kedaluwarsa, salah dimasukkan, atau tidak diperoleh dari registrar Anda saat ini.

Untuk menyelesaikan masalah ini:

- Hubungi registrar Anda saat ini untuk meminta kode otorisasi baru. Pastikan untuk menanyakan berapa lama kode akan tetap aktif sehingga Anda dapat menyelesaikan transfer sebelum kedaluwarsa.
- Ketika Anda menerima kode baru, verifikasi bahwa itu berbeda dari kode sebelumnya. Jika sama, minta registrar Anda untuk menyegarkan atau membuat ulang kode otorisasi.
- Periksa kembali apakah Anda memasukkan kode persis seperti yang disediakan, termasuk huruf besar atau kecil, angka, dan karakter khusus.

“Transfer email otorisasi tidak diterima” atau “batas waktu otorisasi”

Kesalahan ini terjadi ketika Anda tidak mengklik tautan otorisasi di email konfirmasi transfer dalam jangka waktu yang diperlukan (biasanya 5 hari). ICANN memerlukan langkah otorisasi ini untuk semua transfer domain.

Jika Anda tidak menerima email otorisasi atau melewati tenggat waktu, periksa hal berikut:

- Periksa folder spam atau junk mail Anda. Email otorisasi transfer terkadang disaring oleh penyedia email.
- Pastikan kotak pesan Anda tidak penuh dan tidak memiliki batasan penyimpanan yang dapat mencegah pengiriman email.
- Periksa apakah penyedia email Anda memiliki kebijakan yang memfilter email masuk dari pengirim yang tidak dikenal.
- Konfirmasikan bahwa Anda dapat mengakses akun email pendaftar dan alamat email tersebut masih aktif.

Jika perlu, perbarui informasi kontak Anda dengan registrar Anda saat ini sebelum meminta transfer lain. Untuk informasi tentang mengirim ulang email otorisasi, lihat [Mengirim ulang email otorisasi dan konfirmasi](#)

“Domain dikunci” atau “Transfer dilarang”

Kesalahan ini menunjukkan bahwa domain Anda memiliki kunci yang diaktifkan yang mencegah transfer. Sebagian besar pendaftar mengaktifkan kunci domain secara default sebagai tindakan keamanan untuk mencegah transfer yang tidak sah.

Untuk mengatasi masalah ini, masuk ke akun Anda dengan registrar Anda saat ini dan nonaktifkan pengaturan kunci domain atau transfer kunci. Langkah-langkah yang tepat bervariasi menurut

pendaftar, tetapi Anda biasanya akan menemukan pengaturan ini di pengaturan manajemen domain atau keamanan Anda. Jika Anda memerlukan bantuan untuk menemukan pengaturan ini, hubungi pencatat Anda saat ini untuk mendapatkan bantuan.

“Diperlukan verifikasi informasi kontak”

Kesalahan ini terjadi ketika Anda baru saja mengubah informasi kontak domain Anda. Aturan ICANN memerlukan masa tunggu 60 hari setelah perubahan kontak sebelum domain dapat ditransfer untuk mencegah transfer penipuan.

Untuk mengatasi masalah ini, Anda memiliki dua opsi:

- Tunggu 60 hari sejak tanggal perubahan kontak sebelum mencoba transfer lagi.
- Hubungi registrar Anda saat ini untuk memverifikasi informasi kontak Anda saat ini. Beberapa pendaftar dapat mengizinkan Anda untuk memilih keluar dari pembatasan 60 hari jika Anda dapat memverifikasi identitas Anda.

Note

Jika Anda menerima pesan galat yang tidak tercantum di sini, hubungi AWS Support dan sertakan teks kesalahan yang tepat. Tim dukungan kami dapat membantu Anda mendiagnosis dan menyelesaikan masalah transfer khusus untuk situasi Anda.

Saya mengubah pengaturan DNS, tetapi mereka belum diterapkan

Jika Anda mengubah pengaturan DNS, berikut adalah beberapa alasan umum bahwa perubahan belum diterapkan.

Topik

- [Anda mentransfer layanan DNS ke Amazon Route 53 dalam 48 jam terakhir, sehingga DNS masih menggunakan layanan DNS Anda sebelumnya](#)
- [Anda baru saja mentransfer layanan DNS ke Amazon Route 53, tetapi Anda tidak memperbarui server nama dengan registrar domain](#)
- [DNS resolver masih menggunakan pengaturan lama untuk catatan](#)
- [Anda memiliki lebih dari satu zona yang di-hosting dengan nama yang sama, dan Anda memperbarui salah satu yang tidak terkait dengan domain](#)

Anda mentransfer layanan DNS ke Amazon Route 53 dalam 48 jam terakhir, sehingga DNS masih menggunakan layanan DNS Anda sebelumnya

Ketika Anda mentransfer layanan DNS ke Amazon Route 53, Anda menggunakan metode yang disediakan oleh registrar untuk domain Anda untuk mengganti server nama untuk layanan DNS sebelumnya dengan empat server nama untuk Route 53.

 Note

Jika Anda tidak yakin melakukan bagian ini, lihat [Anda baru saja mentransfer layanan DNS ke Amazon Route 53, tetapi Anda tidak memperbarui server nama dengan registrar domain.](#)

Registrar domain biasanya menggunakan TTL (waktu untuk tayang) 24 hingga 48 jam untuk server nama. Ini berarti bahwa ketika DNS resolver mendapatkan server nama untuk domain Anda, ia menggunakan informasi tersebut hingga 48 jam sebelum mengirimkan permintaan lain untuk server nama saat ini untuk domain. Jika Anda mentransfer layanan DNS ke Route 53 dalam 48 jam terakhir dan kemudian mengubah pengaturan DNS, beberapa penyelesaian DNS masih menggunakan layanan DNS lama Anda untuk merutekan lalu lintas untuk domain.

Anda baru saja mentransfer layanan DNS ke Amazon Route 53, tetapi Anda tidak memperbarui server nama dengan registrar domain

Registrar untuk domain Anda memiliki berbagai informasi tentang domain, termasuk server nama untuk layanan DNS untuk domain tersebut. Biasanya, registrar domain juga merupakan layanan DNS Anda, sehingga server nama yang terkait dengan domain Anda milik registrar. Server nama ini memberi tahu DNS tempat mendapatkan informasi tentang cara Anda ingin lalu lintas agar domain Anda dirutekan, misalnya ke alamat IP server web untuk domain Anda.

Saat Anda mentransfer layanan DNS ke Amazon Route 53, Anda perlu menggunakan metode yang disediakan oleh pencatat domain Anda untuk mengubah server nama yang terkait dengan domain Anda. Anda biasanya mengganti server nama yang disediakan oleh registrar dengan empat server nama Route 53 yang terkait dengan zona yang di-hosting yang Anda buat untuk domain.

Jika Anda membuat zona yang di-hosting baru dan catatan untuk domain Anda dan menetapkan pengaturan yang berbeda dari yang Anda gunakan untuk layanan DNS sebelumnya, dan jika DNS

masih merutekan lalu lintas ke sumber daya lama, mungkin Anda tidak memperbarui server nama dengan registrar domain. Untuk menentukan apakah registrar menggunakan server nama untuk zona yang di-hosting Route 53 dan, jika perlu, untuk memperbarui server nama untuk domain, lakukan prosedur berikut:

Untuk mendapatkan server nama untuk zona yang di-hosting Anda dan memperbarui pengaturan server nama dengan registrar domain

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Hosted Zones (Zona yang di-hosting).
3. Pada halaman Hosted Zones (Zona yang di-hosting), pilih nama zona yang di-hosting (bukan tombol radio) untuk zona yang di-hosting.

 Important

Jika Anda memiliki lebih dari satu zona yang di-hosting dengan nama yang sama, pastikan Anda mendapatkan server nama untuk zona yang di-hosting yang benar.

4. Pada daftar Nama catatan, buat catatan dari empat server yang terdaftar untuk Server Nama.
5. Dengan menggunakan metode yang disediakan oleh registrar untuk domain, tampilkan daftar server nama untuk domain tersebut.
6. Jika server nama untuk domain sesuai dengan server nama yang Anda dapatkan di langkah 4, maka konfigurasi domain sudah benar.

Jika server nama untuk domain tidak cocok dengan server nama yang Anda dapatkan di langkah 4, perbarui domain untuk menggunakan server nama Route 53.

7.

 Important

Ketika Anda mengubah nama server untuk domain nama server dari zona yang di-hosting Route 53, ini dapat memakan waktu hingga dua hari untuk perubahan berlaku dan Route 53 untuk menjadi layanan DNS Anda. Ini karena DNS resolver di internet biasanya meminta server nama hanya sekali setiap dua hari dan menyimpan jawabannya.

DNS resolver masih menggunakan pengaturan lama untuk catatan

Jika Anda mengubah pengaturan dalam catatan tetapi lalu lintas Anda masih dialihkan ke sumber daya lama, seperti server web untuk situs web Anda, salah satu kemungkinan penyebabnya adalah DNS masih memiliki pengaturan sebelumnya yang di-cache. Setiap catatan memiliki nilai TTL (waktu untuk tayang (TTL) yang menentukan berapa lama, dalam detik, Anda ingin DNS resolver menyimpan informasi dalam catatan, seperti alamat IP untuk server web. Sampai jumlah waktu yang ditentukan oleh TTL berlalu, DNS resolver akan terus menghasilkan nilai lama dalam menanggapi permintaan DNS. Jika Anda ingin tahu apa TTL adalah untuk catatan, lakukan prosedur berikut.

Note

Untuk catatan alias, TTL ditentukan oleh AWS sumber daya yang dituju oleh catatan rute lalu lintas. Untuk informasi selengkapnya, lihat [Memilih antara catatan alias dan nonalias](#).

Untuk melihat TTL sebagai catatan

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada halaman Hosted Zones (Zona yang di-hosting), pilih nama zona yang di-hosting yang menyertakan catatan.
3. Dalam daftar catatan, temukan catatan yang Anda inginkan untuk nilai TTL, dan periksa nilai pada kolom TTL.

Note

Mengubah TTL sekarang tidak akan membuat perubahan Anda berlaku lebih cepat. DNS resolver sudah memiliki nilai yang di-cache, dan mereka tidak akan mendapatkan pengaturan baru sampai jumlah waktu yang ditentukan oleh pengaturan lama berlalu.

Anda memiliki lebih dari satu zona yang di-hosting dengan nama yang sama, dan Anda memperbarui salah satu yang tidak terkait dengan domain

Anda dapat membuat lebih dari satu zona yang di-hosting yang memiliki nama yang sama, baik menggunakan akun yang sama atau menggunakan beberapa akun. Untuk menentukan

zona host yang digunakan Route 53 untuk merutekan lalu lintas internet untuk domain Anda, Anda mendapatkan empat server nama Route 53 untuk zona yang dihosting tersebut, dan Anda memperbarui pendaftaran domain untuk menggunakan server nama tersebut.

Jika Anda menambahkan, mengubah, atau menghapus catatan dalam satu zona yang di-hosting tetapi pendaftaran domain Anda menggunakan server nama untuk zona yang di-hosting lain, tanggapan Route 53 untuk kueri DNS tidak akan mencerminkan perubahan Anda. Untuk menentukan apakah pendaftaran domain Anda menggunakan server nama untuk zona yang di-hosting tempat Anda memperbarui catatan, lakukan tugas berikut:

1. Tentukan server nama mana yang terkait dengan pendaftaran domain Anda. Lihat [Menambahkan atau mengubah nama server atau glue record](#).
2. Bandingkan server nama yang Anda dapatkan di langkah 1 dengan server nama yang ditetapkan oleh Route 53 ke zona yang di-hosting tempat Anda memperbarui catatan. Lihat [Mendapatkan server nama untuk zona yang di-hosting publik](#).

Jika server nama untuk pendaftaran domain tidak cocok dengan server nama untuk zona yang di-hosting tempat Anda memperbarui catatan, Anda memiliki dua opsi:

Mengubah catatan di zona yang di-hosting yang saat ini terkait dengan domain (disarankan)

Mencatat perubahan yang Anda buat di zona yang di-hosting yang saat ini tidak terkait dengan pendaftaran domain Anda. Kemudian buka zona yang di-hosting yang dikaitkan dengan pendaftaran domain, dan buat perubahan yang sama. Ini adalah metode yang disukai karena perubahan segera berlaku. Untuk informasi selengkapnya, lihat [Mengedit catatan](#).

Perbarui pendaftaran domain Anda untuk menggunakan server nama yang berbeda

Ubah pendaftaran domain Anda untuk menggunakan server nama di zona yang di-hosting yang diperbarui.

Important

Jika Anda mengubah server nama yang terkait dengan pendaftaran domain, domain Anda tidak akan tersedia di internet hingga 2 hari. Ini karena DNS resolver biasanya men-cache nama server nama selama 2 hari. Untuk gambaran umum tentang cara kerja DNS, termasuk informasi tentang resolver cache, lihat [Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda](#).

Dengan mengubah server nama yang terkait dengan pendaftaran domain, Anda pada dasarnya mengubah layanan DNS untuk domain tersebut. Anda memiliki dua pilihan, tergantung apakah domain saat ini sedang digunakan:

- Jika domain sedang digunakan, lihat [Membuat Route 53 sebagai layanan DNS untuk domain yang sedang digunakan](#).
- Jika domain saat ini tidak aktif, lakukan tugas berikut:
 1. Dapatkan server nama untuk zona yang di-hosting yang ingin Anda gunakan untuk merutekan lalu lintas ke domain Anda. Lihat [Mendapatkan server nama untuk zona yang di-hosting publik](#).
 2. Di zona yang di-hosting tempat Anda mendapatkan server nama pada langkah 1, konfirmasi bahwa data NS menggunakan empat server nama yang sama. Jika tidak, perbarui catatan NS. Lihat [Mengedit catatan](#).
 3. Perbarui pendaftaran domain untuk menggunakan server nama yang Anda temukan di langkah 1. Lihat [Menambahkan atau mengubah nama server atau glue record](#).

Peramban saya menampilkan kesalahan "Server tidak ditemukan"

Jika peramban Anda menampilkan kesalahan "Server tidak ditemukan" saat Anda mencoba menjelajah ke domain (example.com) atau subdomain (www.example.com), berikut adalah beberapa penjelasan umum.

Topik

- [Anda tidak membuat data untuk nama domain atau subdomain](#)
- [Anda membuat catatan, tetapi menentukan nilai yang salah](#)
- [Sumber daya tempat Anda mengarahkan lalu lintas tidak tersedia](#)

Anda tidak membuat data untuk nama domain atau subdomain

Jika Anda tidak membuat catatan untuk domain atau subdomain, DNS tidak tahu di mana harus merutekan lalu lintas saat seseorang memasukkan nama tersebut di peramban. Untuk informasi selengkapnya, lihat [Bekerja dengan catatan](#).

Anda membuat catatan, tetapi menentukan nilai yang salah

Saat Anda membuat catatan, mudah untuk menentukan nilai yang salah, seperti alamat IP untuk server web atau nama domain yang CloudFront ditetapkan untuk distribusi web Anda. Jika catatan ada tetapi Anda masih mendapatkan kesalahan "Server tidak ditemukan", kami sarankan Anda mengonfirmasi bahwa nilainya benar.

Sumber daya tempat Anda mengarahkan lalu lintas tidak tersedia

Jika catatan menentukan sumber daya seperti server web yang tidak tersedia, peramban akan menghasilkan kesalahan "Server tidak ditemukan". Sebaiknya Anda memeriksa status sumber daya yang menjadi tujuan perutean lalu lintas.

Saya tidak dapat merutekan lalu lintas ke bucket Amazon S3 yang dikonfigurasi untuk meng-host situs web

Saat Anda mengonfigurasi bucket Amazon S3 untuk meng-host situs web, Anda harus memberi nama yang sama pada bucket dengan catatan yang ingin Anda gunakan untuk merutekan lalu lintas ke bucket. Misalnya, jika Anda ingin merutekan lalu lintas untuk example.com ke bucket S3 yang dikonfigurasi untuk meng-host situs web, nama bucket harus example.com.

Jika Anda ingin merutekan lalu lintas ke bucket S3 yang dikonfigurasi untuk hosting situs web tetapi nama bucket tidak muncul di daftar Target Alias di konsol Amazon Route 53, atau jika Anda mencoba membuat catatan alias secara terprogram dan Anda mendapatkan InvalidInput kesalahan dari API Route 53, salah satunya, atau AWS SDKs AWS CLI AWS Tools for Windows PowerShell, periksa hal berikut:

- Nama bucket sama persis dengan nama catatan, seperti example.com atau www.example.com.
- Bucket S3 dikonfigurasi dengan benar untuk meng-host situs web. Untuk informasi selengkapnya, lihat [Hosting situs web statis di Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Saya ditagih dua kali untuk zona yang di-hosting yang sama

Kami tidak menagih Anda jika Anda menghapus zona yang di-hosting dalam waktu 12 jam setelah Anda membuatnya. Setelah 12 jam, kami segera mengenakan biaya bulanan standar untuk zona

yang di-hosting. Biaya bulanan untuk zona yang di-hosting tidak prorata untuk bulan parsial. (Biaya yang sama berlaku untuk zona yang di-hosting yang secara otomatis kami buat saat Anda mendaftarkan domain.)

Jika Anda membuat zona yang di-hosting pada hari terakhir bulan (misalnya, 31 Januari), biaya untuk Januari mungkin muncul pada faktur Februari, bersama dengan biaya untuk Februari. Perhatikan bahwa Amazon Route 53 menggunakan Waktu Universal Terkoordinasi (UTC) sebagai zona waktu untuk menentukan kapan zona yang di-hosting dibuat.

Saya ditagih beberapa faktur untuk domain saya

Saat Anda mendaftar untuk berlangganan, membayar biaya pendaftaran, biaya transfer, atau biaya perpanjangan dengan biaya di muka, faktur unik dihasilkan. Faktur ini tetap ada di konsol Penagihan, bahkan jika transaksi pembayaran tidak berhasil. Item baris penagihan terkait ditampilkan sebagai [x] Kuantitas di bawah sub-bagian Registrar-Global pada tab Detail Tagihan berdasarkan layanan di konsol Penagihan.

Untuk melihat faktur yang dibebaskan, selesaikan langkah-langkah berikut:

Untuk melihat faktur yang dibebaskan di konsol Penagihan

1. Masuk ke Konsol Manajemen AWS dan buka AWS Billing and Cost Management konsol di <https://console.aws.amazon.com/costmanagement/>.
2. Di panel navigasi, pilih Tagihan.
3. Pilih Faktur untuk melihat detail faktur yang dibebaskan.

Untuk melihat pembayaran dan pengembalian dana yang berhasil di konsol Penagihan, selesaikan langkah-langkah berikut:

Untuk mengkonfirmasi pembayaran atau pengembalian uang yang berhasil diproses

1. Di panel navigasi, pilih Pembayaran.
2. Pilih tab Transaksi untuk melihat tabel Transaksi untuk semua transaksi yang diselesaikan AWS.

AWS Akun saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53

Jika Anda menutup AWS akun Anda, atau jika akun Anda ditutup atau ditutup secara permanen, domain Anda akan melalui proses penghapusan:

1. Kami akan memberi tahu Anda bahwa akun Anda ditutup dan domain Anda akan ditangguhkan dalam 5 hari ke depan setiap hari.
2. Setelah domain Anda ditangguhkan, berikut ini akan terjadi:
 - Jika registrar Anda adalah Amazon Registrar, kami akan memberi tahu Anda bahwa kami akan menghapus domain Anda dalam 30 hari. Untuk informasi selengkapnya, lihat [Menemukan registrar Anda dan informasi lain tentang domain Anda](#).
 - Jika registrar Anda adalah Gandi, kami akan memberi tahu Anda bahwa kami akan merilis domain Anda ke Gandi ketika akun Anda ditutup secara permanen.
3. Setelah menunggu 30 hari, kami akan menghapus semua domain yang terdaftar di Amazon Registrar di akun dan mengirimkan Anda pembaruan.
4. Ketika akun Anda ditutup secara permanen, kami akan merilis semua domain yang terdaftar di Gandi di akun ke Gandi.

Jika Anda membuka kembali akun selama periode waktu domain Anda dapat dipulihkan, kami akan membatalkan penangguhan domain Anda, atau memberi tahu Anda bahwa domain Anda telah dihapus tetapi domain tersebut mungkin dapat dipulihkan. Untuk informasi selengkapnya, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

Note

Setelah 90 hari berlalu sejak Anda menutup akun, Anda tidak dapat lagi membukanya kembali. Untuk informasi selengkapnya, lihat [Menutup AWS akun](#) di panduan Manajemen Akun.

Lihat informasi yang lebih lengkap di [Menghubungi AWS Support tentang masalah pendaftaran domain](#).

Rentang alamat IP server Amazon Route 53

Amazon Web Services (AWS) menerbitkan rentang alamat IP saat ini dalam format JSON.

Jika firewall atau grup keamanan membatasi lalu lintas masuk berdasarkan alamat IP sumber, konfirmasi bahwa konfigurasi Anda mengizinkan lalu lintas dari rentang alamat IP yang berlaku.

Untuk melihat rentang alamat IP Route 53 saat ini, unduh [ip-ranges.json](#), dan cari file untuk nilai berikut:

- "service": "ROUTE53"
- "service": "ROUTE53_HEALTHCHECKS"
- "service": "ROUTE53_HEALTHCHECKS_PUBLISHING"

Untuk informasi selengkapnya tentang alamat IP untuk AWS sumber daya, lihat [rentang alamat AWS IP](#) di Referensi Umum Amazon Web Services.

Rentang alamat IP dari server nama Route 53

"service": "ROUTE53"— Rentang alamat IP ini digunakan oleh server nama Route 53.

Tambahkan rentang ini ke daftar rentang alamat IP yang diizinkan jika Anda menggunakan Route 53 sebagai layanan DNS untuk satu atau beberapa domain dan Anda ingin dapat menggunakan perintah dig atau nslookup untuk membuat kueri server nama Route 53.

Note

Alamat IP server nama Route 53 bersifat statis.

Rentang alamat IP pemeriksaan kesehatan Route 53

"service": "ROUTE53_HEALTHCHECKS"— Rentang alamat IP ini digunakan oleh pemeriksa kesehatan Route 53. Tambahkan rentang ini ke daftar rentang alamat IP yang diizinkan jika Anda menggunakan pemeriksaan kondisi Route 53 untuk memeriksa kondisi sumber daya di jaringan Anda.

 Note

Kami jarang mengubah rentang alamat IP pemeriksaan kesehatan. Pantau file [ip-ranges.json](#) untuk pembaruan apa pun pada rentang ini.

Untuk informasi selengkapnya tentang alamat IP untuk pemeriksaan kondisi, lihat [Mengonfigurasi aturan router dan firewall untuk pemeriksaan kondisi Amazon Route 53](#).

Mereferensikan daftar awalan

Daftar awalan adalah sekumpulan satu atau beberapa entri blok CIDR yang dapat Anda gunakan untuk mengonfigurasi grup keamanan. Router dan firewall Anda untuk aturan untuk EC2 instans Amazon harus mengizinkan lalu lintas masuk dari alamat IP yang digunakan pemeriksaan kesehatan Route 53. Referensi ke daftar awalan membantu Anda menyederhanakan pengelolaan blok CIDR dalam aturan Anda. Jika Anda sering menggunakan aturan yang sama CIDRs di beberapa aturan, Anda dapat mengelolanya CIDRs dalam satu daftar awalan, alih-alih berulang kali mereferensikan hal yang sama CIDRs di setiap aturan. Jika Anda perlu menghapus blok CIDR, Anda dapat menghapus entri dari daftar awalan alih-alih menghapus CIDR dari setiap aturan yang terpengaruh. Untuk informasi selengkapnya tentang daftar awalan secara umum, lihat [mengelompokkan blok CIDR menggunakan daftar awalan terkelola di Panduan Pengguna Amazon VPC](#).

AWS Daftar awalan terkelola adalah kumpulan rentang alamat IP untuk AWS layanan. AWS Daftar awalan terkelola dibuat dan dikelola oleh AWS dan dapat digunakan oleh siapa saja yang memiliki akun AWS . Anda tidak dapat membuat, memodifikasi, membagikan, atau menghapus daftar awalan yang AWS dikelola.

Untuk informasi selengkapnya tentang daftar awalan AWS-terkelola, lihat [Bekerja dengan daftar awalan AWS-terkelola di Panduan Pengguna Amazon VPC](#).

Rentang alamat IP internal pemeriksaan kesehatan Route 53

"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"—. Route 53 menggunakan rentang alamat IP ini hanya secara internal. Anda tidak perlu menambahkan rentang ini ke daftar rentang yang diizinkan.

Memberi tanda pada sumber daya Amazon Route 53

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri atas sebuah kunci dan sebuah nilai, yang keduanya Anda tentukan. Misalnya, kunci dapat berupa "domain" dan nilai dapat berupa "contoh.com". Anda dapat menggunakan tanda untuk berbagai tujuan; satu penggunaan umum adalah untuk mengategorikan dan melacak Anda Amazon Route 53 biaya. Saat Anda menerapkan tag ke zona, domain, dan pemeriksaan kesehatan yang dihosting Route 53 AWS, buat laporan alokasi biaya sebagai file nilai dipisahkan koma (CSV) dengan penggunaan dan biaya yang dikumpulkan berdasarkan tag Anda. Anda dapat menerapkan tanda yang mewakili kategori bisnis (seperti pusat biaya, nama aplikasi, atau pemilik) untuk mengatur biaya Anda di berbagai layanan. Untuk informasi selengkapnya tentang penggunaan tanda untuk alokasi biaya, lihat [Menggunakan Tanda Alokasi Biaya](#) dalam [Panduan Pengguna AWS Billing](#).

Untuk kemudahan penggunaan dan hasil terbaik, gunakan Editor Tag di Konsol Manajemen AWS, yang menyediakan cara terpusat dan terpadu untuk membuat dan mengelola tag Anda. Untuk informasi selengkapnya, lihat [Cara menggunakan Editor Tanda](#) dalam [Memulai dengan Konsol Manajemen AWS](#). Anda juga dapat menggunakan konsol Route 53 untuk menerapkan tanda untuk beberapa sumber daya:

- Pemeriksaan kondisi – Untuk informasi lebih lanjut, lihat [Penamaan dan penandaan pemeriksaan kondisi](#).
- Route 53 VPC Resolver titik akhir masuk — Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#)
- Titik akhir resolver outbound – Untuk informasi lebih lanjut, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar](#).
- Aturan Resolver – Untuk informasi lebih lanjut, lihat: [Nilai yang Anda tentukan ketika membuat atau mengedit aturan](#).
- Zona yang dihosting — Untuk informasi lebih lanjut, lihat [Bekerja dengan zona yang di-hosting](#).

Note

Biaya untuk titik akhir Resolver dialokasikan per antarmuka jaringan VPC Resolver. Karena saat ini tidak mungkin untuk menandai antarmuka jaringan VPC Resolver, alokasi biaya berbasis tag saat ini tidak didukung untuk titik akhir Resolver. Untuk informasi tentang harga untuk Resolver VPC, lihat harga [Amazon](#) Route 53.

Anda juga dapat menerapkan tanda ke sumber daya dengan menggunakan API Route 53. Untuk informasi lebih lanjut, lihat tindakan yang terkait dengan tanda dalam topik [tindakan API Route 53 berdasarkan fungsi](#) di Referensi Amazon Route 53.

Tutorial

Bagian ini mencakup tutorial berikut:

Menggunakan Route 53 sebagai layanan DNS untuk subdomain

Pelajari cara menggunakan Route 53 sebagai layanan DNS untuk subdomain baru atau yang sudah ada saat masih menggunakan layanan DNS lain untuk domain induk.

Transisi ke perutean berbasis Latensi

Temukan cara bermigrasi secara bertahap dari perutean standar ke perutean berbasis latensi di Route 53, mengarahkan pengguna ke titik akhir latensi terendah yang tersedia. AWS

Gabungkan catatan tertimbang dan latensi untuk transisi yang mulus dan berisiko rendah dengan kontrol penuh dan kemampuan rollback.

Menambahkan Wilayah lain ke perutean berbasis latensi

Perluas pengaturan perutean berbasis latensi Anda dengan menambahkan AWS Wilayah baru dan secara bertahap mengalihkan lalu lintas ke Wilayah baru.

Merutekan lalu lintas ke beberapa EC2 instans Amazon di suatu Wilayah

Gunakan kombinasi latensi dan catatan tertimbang untuk merutekan lalu lintas ke EC2 beberapa instans Amazon dalam instans tertentu. Wilayah AWS

Mengelola lebih dari 100 catatan tertimbang

Pelajari cara mengarahkan lalu lintas ke lebih dari 100 titik akhir dengan membuat pohon catatan alias tertimbang dan catatan tertimbang.

Menimbang jawaban multi-record yang toleran terhadap kesalahan

Pahami cara menimbang respons DNS yang berisi banyak catatan, memberikan toleransi kesalahan dan penyeimbangan beban di beberapa titik akhir.

Tutorial ini mencakup berbagai kasus penggunaan dan skenario, membantu Anda secara efektif memanfaatkan kebijakan perutean Route 53, catatan tertimbang, dan perutean berbasis latensi untuk mengoptimalkan manajemen DNS dan perutean lalu lintas Anda.

Topik

- [Menggunakan Amazon Route 53 sebagai layanan DNS untuk subdomain tanpa memigrasi domain induk](#)
- [Transisi ke latensi berbasis perutean di Amazon Route 53](#)
- [Menambahkan Wilayah lain untuk perutean berbasis latensi Anda di Amazon Route 53](#)
- [Menggunakan latensi dan catatan tertimbang di Amazon Route 53 untuk merutekan lalu lintas ke EC2 beberapa instans Amazon di suatu Wilayah](#)
- [Mengelola lebih 100 catatan tertimbang di Amazon Route 53](#)
- [Menimbang jawaban multicatatan yang toleran terhadap kesalahan di Amazon Route 53](#)

Menggunakan Amazon Route 53 sebagai layanan DNS untuk subdomain tanpa memigrasi domain induk

Amazon Route 53 memberikan fleksibilitas dalam mengelola DNS untuk subdomain, memungkinkan Anda memanfaatkan fitur-fiturnya tanpa perlu memigrasikan seluruh domain induk.

Anda dapat membuat subdomain baru atau memigrasikan subdomain yang sudah ada ke Route 53, sambil menjaga domain induk dihosting dengan penyedia layanan DNS lain.

Membuat subdomain baru dengan Route 53:

1. Buat zona yang dihosting untuk subdomain baru.
2. Tambahkan catatan DNS yang diinginkan (misalnya, A, CNAME, MX) untuk subdomain ke zona yang dihosting.
3. Dapatkan server nama Route 53 yang ditetapkan ke zona yang dihosting.
4. Perbarui konfigurasi DNS domain induk dengan menambahkan catatan NS (Name Server) untuk subdomain, menunjuk ke server nama Route 53.

Migrasi subdomain yang ada ke Route 53:

1. Membuat zona yang di-hosting untuk subdomain.
2. Dapatkan konfigurasi DNS saat ini untuk subdomain dari penyedia layanan DNS Anda yang ada.
3. Tambahkan catatan DNS yang sesuai ke zona yang dihosting.
4. Dapatkan server nama Route 53 yang ditetapkan ke zona yang dihosting.

5. Perbarui konfigurasi DNS domain induk dengan menambahkan catatan NS untuk subdomain, menunjuk ke server nama Route 53.

Dengan mengikuti langkah-langkah ini, Anda dapat memanfaatkan fitur-fitur lanjutan Route 53, seperti pemeriksaan kesehatan, kebijakan perutean, dan manajemen arus lalu lintas, untuk subdomain Anda sambil mempertahankan konfigurasi DNS domain induk dengan penyedia yang ada.

Topik

- [Membuat subdomain yang menggunakan Amazon Route 53 sebagai layanan DNS tanpa memigrasi domain induk](#)
- [Memigrasi layanan DNS untuk subdomain ke Amazon Route 53 tanpa memigrasi domain induk](#)

Membuat subdomain yang menggunakan Amazon Route 53 sebagai layanan DNS tanpa memigrasi domain induk

Anda dapat membuat subdomain yang menggunakan Amazon Route 53 sebagai layanan DNS tanpa migrasi domain induk dari layanan DNS lain.

Proses ini memiliki langkah-langkah dasar berikut:

1. [Cari tahu](#) apakah Anda bahkan harus menggunakan prosedur ini.
2. [Membuat zona yang di-hosting Route 53 untuk subdomain.](#)
3. [Tambahkan catatan](#) untuk subdomain baru ke zona yang di-hosting Route 53.
4. API saja: [Konfirmasikan bahwa perubahan Anda telah disebar](#) untuk semua server DNS Route 53.

Note

Saat ini, satu-satunya cara untuk memverifikasi bahwa perubahan telah disebar adalah dengan menggunakan tindakan [GetChangeAPI](#). Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

5. [Perbarui layanan DNS untuk domain induk dengan menambahkan nama server catatan untuk subdomain.](#)

Memutuskan prosedur mana yang akan digunakan untuk membuat subdomain

Prosedur dalam topik ini menjelaskan cara melakukan operasi yang tidak biasa. Jika Anda sudah menggunakan Route 53 sebagai layanan DNS untuk domain Anda dan Anda hanya ingin merutekan lalu lintas untuk subdomain, seperti `www.example.com`, ke sumber daya Anda, seperti server web yang berjalan pada sebuah instance, lihat. EC2 [Merutekan lalu lintas untuk subdomain](#)

Gunakan prosedur ini hanya jika Anda menggunakan layanan DNS lain untuk domain, misalnya `example.com`, dan Anda ingin mulai menggunakan Route 53 sebagai layanan DNS untuk subdomain baru domain tersebut, misalnya `www.example.com`.

Membuat zona yang di-hosting untuk subdomain baru

Bila Anda ingin menggunakan Amazon Route 53 sebagai layanan DNS untuk subdomain baru tanpa memigrasi domain induk, Anda mulai dengan membuat zona yang di-hosting untuk subdomain. Route 53 menyimpan informasi tentang subdomain Anda di zona yang di-hosting.

Untuk informasi tentang cara membuat zona yang di-hosting menggunakan konsol Route 53, lihat [Membuat zona yang di-hosting publik](#).

Membuat catatan

Anda dapat membuat catatan menggunakan konsol Amazon Route 53 atau API Route 53. Catatan yang Anda buat di Route 53 akan menjadi catatan yang digunakan DNS setelah Anda mendelegasikan tanggung jawab untuk subdomain ke Route 53, seperti yang dijelaskan di [Memperbarui layanan DNS Anda dengan catatan server nama untuk subdomain](#), nanti saat proses berlangsung.

Important

Jangan membuat catatan name server (NS) atau start of authority (SOA) tambahan di zona yang di-hosting Route 53, dan jangan hapus catatan NS dan SOA yang ada.

Untuk membuat catatan menggunakan konsol Route 53, lihat [Bekerja dengan catatan](#). Untuk membuat catatan menggunakan API Route 53, gunakan `ChangeResourceRecordSets`. Untuk informasi selengkapnya, lihat [ChangeResourceRecordSets](#) di [Referensi API Amazon Route 53](#).

Memeriksa status perubahan Anda (hanya API)

Membuat zona yang di-hosting baru dan mengubah catatan membutuhkan waktu untuk menyebarkan ke server DNS Route 53. Jika Anda biasa [ChangeResourceRecordSets](#) membuat catatan, Anda dapat menggunakan `GetChange` tindakan untuk menentukan apakah perubahan Anda telah disebarkan. (`ChangeResourceRecordSets` mengembalikan nilai untuk `ChangeId`, yang dapat Anda sertakan dalam `GetChange` permintaan berikutnya. `ChangeId` tidak tersedia jika Anda membuat catatan dengan menggunakan konsol.) Untuk informasi selengkapnya, lihat [GET GetChange](#) di Referensi API Amazon Route 53.

Note

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Memperbarui layanan DNS Anda dengan catatan server nama untuk subdomain

Setelah perubahan catatan Amazon Route 53 telah disebarkan (lihat [Memeriksa status perubahan Anda \(hanya API\)](#)), perbarui layanan DNS untuk domain induk dengan menambahkan catatan NS untuk subdomain. Hal ini dikenal sebagai mendelegasikan tanggung jawab untuk subdomain untuk Route 53. Misalnya, jika domain induk `example.com` di-hosting dengan layanan DNS lain dan Anda membuat subdomain `test.example.com` di Route 53, Anda harus memperbarui layanan DNS untuk `example.com` dengan catatan NS baru untuk `test.example.com`.

Lakukan prosedur berikut.

1. Menggunakan metode yang disediakan oleh layanan DNS Anda, cadangkan file zona untuk domain induk.
2. Di konsol Route 53, dapatkan server nama untuk zona yang di-hosting Route 53:
 - a. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 - b. Dalam panel navigasi, klik Zona yang di-hosting.
 - c. Pada halaman Zona yang di-hosting, pilih tombol radio (bukan nama) untuk zona yang di-hosting, lalu pilih Lihat detail.
 - d. Pada halaman detail untuk zona yang di-hosting, pilih Detail zona yang di-hosting.
 - e. Catat empat server yang tercantum untuk Nama server.

Atau, Anda dapat menggunakan tindakan `GetHostedZone`. Untuk informasi selengkapnya, lihat [GetHostedZone](#) di Referensi API Amazon Route 53.

3. Menggunakan metode yang disediakan oleh layanan DNS domain induk, tambahkan catatan NS untuk subdomain ke file zona untuk domain induk. Dalam catatan NS ini, tentukan empat server nama Route 53 yang terkait dengan zona yang di-hosting yang Anda buat di langkah 1.

Important

Jangan tambahkan catatan awal otoritas (SOA) ke file zona untuk domain induk. Karena subdomain akan menggunakan Route 53, layanan DNS untuk domain induk bukanlah otoritas untuk subdomain.

Jika layanan DNS Anda secara otomatis menambahkan catatan SOA untuk subdomain, hapus catatan untuk subdomain. Namun, jangan menghapus catatan SOA untuk domain induk.

Memigrasi layanan DNS untuk subdomain ke Amazon Route 53 tanpa memigrasi domain induk

Anda dapat memigrasi subdomain untuk menggunakan Amazon Route 53 sebagai layanan DNS tanpa migrasi domain induk dari layanan DNS lain.

Proses ini memiliki langkah-langkah dasar berikut:

1. [Cari tahu](#) apakah Anda bahkan harus menggunakan prosedur ini.
2. [Membuat zona yang di-hosting Route 53 untuk subdomain](#).
3. [Dapatkan konfigurasi DNS saat ini dari penyedia layanan DNS saat ini untuk domain induk](#).
4. [Tambahkan catatan catatan](#) Untuk subdomain Anda zona yang di-hosting Route 53.
5. API saja: [Konfirmasikan bahwa perubahan Anda telah disebar](#) untuk semua server DNS Route 53.

 Note

Saat ini, satu-satunya cara untuk memverifikasi bahwa perubahan telah disebar adalah dengan menggunakan tindakan [GetChangeAPI](#). Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

6. [Memperbarui konfigurasi DNS dengan penyedia layanan DNS untuk domain induk dengan menambahkan nama server catatan untuk subdomain.](#)

Memutuskan prosedur mana yang akan digunakan untuk membuat subdomain

Prosedur dalam topik ini menjelaskan cara melakukan operasi yang tidak biasa. Jika Anda sudah menggunakan Route 53 sebagai layanan DNS untuk domain Anda dan Anda hanya ingin merutekan lalu lintas untuk subdomain, seperti `www.example.com`, ke sumber daya Anda, seperti server web yang berjalan pada sebuah instance, lihat. EC2 [Merutekan lalu lintas untuk subdomain](#)

Gunakan prosedur ini hanya jika Anda menggunakan layanan DNS lain untuk domain, misalnya `example.com`, dan Anda ingin mulai menggunakan Route 53 sebagai layanan DNS untuk subdomain yang ada pada domain tersebut, misalnya `www.example.com`.

Membuat zona yang di-hosting untuk subdomain

Jika Anda ingin memigrasi subdomain dari layanan DNS lain ke Amazon Route 53 tetapi Anda tidak ingin memigrasi domain induk, mulai dengan membuat zona yang di-hosting untuk subdomain. Route 53 menyimpan informasi tentang subdomain Anda di zona yang di-hosting.

Untuk informasi tentang cara membuat zona yang di-hosting menggunakan konsol Route 53, lihat [Membuat zona yang di-hosting publik](#).

Mendapatkan konfigurasi DNS Anda saat ini dari penyedia layanan DNS

Untuk menyederhanakan proses migrasi subdomain yang ada ke Route 53, dapatkan konfigurasi DNS saat ini untuk domain dari penyedia layanan DNS yang saat ini melayani domain. Anda dapat menggunakan informasi ini sebagai dasar untuk mengonfigurasi Route 53 sebagai layanan DNS untuk subdomain.

Apa yang Anda minta dan format yang masuk tergantung perusahaan mana yang saat ini Anda gunakan sebagai penyedia layanan DNS Anda. Idealnya, mereka akan memberikan file zona, yang

berisi informasi tentang semua catatan dalam konfigurasi Anda saat ini. (Catatan memberi tahu DNS bagaimana Anda ingin lalu lintas dirutekan untuk domain dan subdomain Anda. Misalnya, ketika seseorang memasukkan nama domain Anda di browser web, apakah Anda ingin lalu lintas diarahkan ke server web di pusat data Anda, ke EC2 instance Amazon, ke CloudFront distribusi, atau ke lokasi lain?) Jika Anda bisa mendapatkan file zona dari penyedia layanan DNS saat ini, Anda dapat mengedit file zona untuk menghapus catatan yang tidak ingin Anda migrasi ke Amazon Route 53. Kemudian Anda dapat mengimpor catatan yang tersisa ke zona yang di-hosting Route 53 Anda, yang menyederhanakan proses dengan signifikan. Coba tanyakan ke dukungan pelanggan untuk penyedia layanan DNS Anda saat ini tentang cara mendapatkan file zona atau daftar catatan.

Membuat catatan

Menggunakan catatan yang Anda dapatkan dari penyedia layanan DNS Anda saat ini sebagai titik awal, buat catatan yang sesuai di zona yang di-hosting Amazon Route 53 yang Anda buat untuk subdomain. Catatan yang Anda buat di Route 53 akan menjadi catatan yang digunakan DNS setelah Anda mendelegasikan tanggung jawab untuk subdomain ke Route 53, seperti yang dijelaskan di [Memperbarui layanan DNS Anda dengan catatan server nama untuk subdomain](#), nanti saat proses berlangsung.

Important

Jangan membuat catatan name server (NS) atau start of authority (SOA) tambahan di zona yang di-hosting Route 53, dan jangan hapus catatan NS dan SOA yang ada.

Untuk membuat catatan menggunakan konsol Route 53, lihat [Bekerja dengan catatan](#). Untuk membuat catatan menggunakan API Route 53, gunakan `ChangeResourceRecordSets`. Untuk informasi selengkapnya, lihat [ChangeResourceRecordSets](#) di [Referensi API Amazon Route 53](#).

Memeriksa status perubahan Anda (hanya API)

Membuat zona yang di-hosting baru dan mengubah catatan membutuhkan waktu untuk menyebarkan ke server DNS Route 53. Jika Anda biasa [ChangeResourceRecordSets](#) membuat catatan, Anda dapat menggunakan `GetChange` tindakan untuk menentukan apakah perubahan Anda telah disebarkan. (`ChangeResourceRecordSets` mengembalikan nilai untuk `ChangeId`, yang dapat Anda sertakan dalam `GetChange` permintaan berikutnya. `ChangeId` tidak tersedia jika Anda membuat catatan dengan menggunakan konsol.) Untuk informasi selengkapnya, lihat [GET GetChange](#) di [Referensi API Amazon Route 53](#).

 Note

Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik.

Memperbarui layanan DNS Anda dengan catatan server nama untuk subdomain

Setelah perubahan catatan Amazon Route 53 telah disebarkan (lihat [Memeriksa status perubahan Anda \(hanya API\)](#)), perbarui layanan DNS untuk domain induk dengan menambahkan catatan NS untuk subdomain. Hal ini dikenal sebagai mendelegasikan tanggung jawab untuk subdomain untuk Route 53. Misalnya, domain induk example.com di-hosting dengan layanan DNS lain dan Anda memigrasi subdomain test.example.com ke Route 53. Anda harus membuat zona yang di-hosting untuk test.example.com dan memperbarui layanan DNS untuk example.com dengan catatan NS yang Route 53 ditugaskan ke zona yang di-hosting baru untuk test.example.com.

Lakukan prosedur berikut.

1. Menggunakan metode yang disediakan oleh layanan DNS Anda, cadangkan file zona untuk domain induk.
2. Jika penyedia layanan DNS sebelumnya untuk domain memiliki metode untuk mengubah pengaturan TTL untuk server nama mereka, kami sarankan Anda mengubah pengaturan menjadi 900 detik. Ini membatasi waktu selama permintaan klien akan mencoba untuk menyelesaikan nama domain menggunakan server nama usang. Jika TTL saat ini 172.800 detik (dua hari), yang merupakan pengaturan default umum, Anda masih perlu menunggu dua hari untuk resolver dan klien untuk menghentikan cache data DNS menggunakan TTL sebelumnya. Setelah pengaturan TTL berakhir, Anda dapat dengan aman menghapus catatan yang disimpan di penyedia sebelumnya dan membuat perubahan hanya untuk Route 53.
3. Di konsol Route 53, dapatkan server nama untuk zona yang di-hosting Route 53:
 - a. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
 - b. Dalam panel navigasi, klik Zona yang di-hosting.
 - c. Pada halaman Zona yang di-hosting, pilih tombol radio (bukan nama) untuk zona yang di-hosting, lalu pilih Lihat detail.
 - d. Pada halaman detail untuk zona yang di-hosting, pilih Detail zona yang di-hosting.
 - e. Catat empat server yang tercantum untuk Nama server.

Atau, Anda dapat menggunakan tindakan `GetHostedZone`. Untuk informasi selengkapnya, lihat [GetHostedZone](#) di Referensi API Amazon Route 53.

4. Menggunakan metode yang disediakan oleh layanan DNS domain induk, tambahkan catatan NS untuk subdomain ke file zona untuk domain induk. Berikan catatan NS nama yang sama dengan subdomain. Untuk nilai dalam catatan NS, tentukan empat server nama Route 53 yang terkait dengan zona yang di-hosting yang Anda buat di langkah 2. Perhatikan bahwa layanan DNS yang berbeda menggunakan terminologi yang berbeda. Anda mungkin perlu menghubungi dukungan teknis untuk layanan DNS Anda guna mempelajari cara melakukan langkah ini.

 Important

Jangan tambahkan catatan awal otoritas (SOA) ke file zona untuk domain induk. Karena subdomain akan menggunakan Route 53, layanan DNS untuk domain induk bukanlah otoritas untuk subdomain.

Jika layanan DNS Anda secara otomatis menambahkan catatan SOA untuk subdomain, hapus catatan untuk subdomain. Namun, jangan menghapus catatan SOA untuk domain induk.

Bergantung pada pengaturan TTL untuk server nama untuk domain induk, penyebaran perubahan Anda ke DNS resolver dapat memakan waktu 48 jam atau lebih. Selama periode ini, DNS resolver masih dapat menjawab permintaan dengan server nama untuk layanan DNS domain induk. Selain itu, komputer klien dapat terus memiliki server nama sebelumnya untuk subdomain di cache mereka.

5. Setelah pengaturan TTL registrar untuk domain kedaluwarsa (lihat Langkah 2), hapus catatan berikut dari file zona untuk domain induk:
 - Catatan yang ditambahkan ke Route 53 seperti yang dijelaskan dalam [Membuat catatan](#).
 - Catatan NS layanan DNS Anda. Setelah Anda selesai menghapus catatan NS, satu-satunya catatan NS di file zona adalah yang Anda buat di Langkah 4.

Transisi ke latensi berbasis perutean di Amazon Route 53

Dengan perutean berbasis latensi, Amazon Route 53 dapat mengarahkan pengguna Anda ke titik akhir latensi terendah yang tersedia. AWS Misalnya, Anda dapat mengaitkan nama DNS seperti

`www.example.com` dengan ELB Classic, Application, atau Network Load Balancer, atau dengan instans EC2 Amazon atau alamat IP Elastis yang di-host di wilayah AS Timur (Ohio) dan Eropa (Irlandia). Server DNS Route 53 memutuskan, berdasarkan kondisi jaringan dalam beberapa minggu terakhir, contoh di wilayah mana yang harus melayani pengguna tertentu. Pengguna di London kemungkinan akan diarahkan ke instans Europe (Ireland), pengguna di Chicago kemungkinan akan diarahkan ke instans US East (Ohio), dan seterusnya. Route 53 mendukung perutean berbasis latensi untuk catatan A, AAAA, TXT, dan CNAME, serta alias untuk catatan A dan AAAA.

Note

Data tentang latensi antara pengguna dan sumber daya Anda sepenuhnya didasarkan pada lalu lintas antara pengguna dan pusat AWS data. Jika Anda tidak menggunakan sumber daya di AWS Wilayah, latensi aktual antara pengguna dan sumber daya dapat sangat bervariasi dari data AWS latensi. Ini benar bahkan jika sumber daya Anda terletak di kota yang sama dengan AWS Wilayah.

Untuk transisi yang mulus dan berisiko rendah, Anda dapat menggabungkan catatan tertimbang dan latensi untuk bermigrasi secara bertahap dari perutean standar ke perutean berbasis latensi dengan kontrol penuh dan kemampuan rollback pada setiap tahap. Mari kita pertimbangkan contoh yang saat `www.example.com` ini di-host di EC2 instans Amazon di wilayah AS Timur (Ohio). Instans ini memiliki alamat IP Elastis `W.W.W.W`. Misalkan Anda ingin melanjutkan perutean lalu lintas ke wilayah AS Timur (Ohio) bila berlaku sementara juga mulai mengarahkan pengguna ke EC2 instance Amazon tambahan di wilayah AS Barat (California N.) (IP Elastis) dan di wilayah Eropa (Irlandia `X.X.X.X`) (IP Elastis). `Y.Y.Y.Y` Zona yang di-hosting Route 53 `example.com` sudah memiliki catatan untuk `www.example.com` yang memiliki Tipe dari A dan Nilai (alamat IP) `W.W.W.W`.

Setelah selesai dengan contoh berikut, Anda akan memiliki dua catatan alias tertimbang:

- Anda akan mengonversi catatan yang ada `www.example.com` menjadi catatan alias tertimbang yang terus mengarahkan sebagian besar lalu lintas Anda ke EC2 instans Amazon yang ada di wilayah AS Timur (Ohio).
- Anda akan membuat catatan alias tertimbang lain yang awalnya hanya mengarahkan sebagian kecil lalu lintas ke catatan latensi Anda, yang mengarahkan lalu lintas ke ketiga wilayah.

Dengan memperbarui bobot dalam catatan alias tertimbang ini, Anda dapat secara bertahap beralih dari lalu lintas perutean hanya ke wilayah AS Timur (Ohio) ke mengarahkan lalu lintas ke ketiga wilayah tempat Anda memiliki instans Amazon. EC2

Untuk beralih ke perutean berbasis latensi

1. Buat salinan catatan untuk `www.example.com`, tetapi gunakan nama domain baru, misalnya, `copy-www.example.com`. Berikan catatan baru Jenis (A) dan Nilai (`W.W.W.W`) yang sama sebagai catatan untuk `www.example.com`.
2. Memperbarui catatan A yang ada untuk `www.example.com` guna membuatnya catatan alias tertimbang:
 - Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), pilih Alias to another record in this hosted zone (Alias ke catatan lain di zona yang di-hosting ini), dan tentukan `copy-www.example.com`.
 - Untuk Bobot, tentukan 100.

Ketika Anda selesai dengan pembaruan, Route 53 akan terus menggunakan catatan ini untuk merutekan semua lalu lintas ke sumber daya yang memiliki alamat IP `W.W.W.W`.

3. Buat catatan latensi untuk setiap EC2 instans Amazon Anda, misalnya:
 - US East (Ohio), Alamat IP Elastis `W.W.W.W`
 - US West (N. California), Alamat IP Elastis `X.X.X.X`
 - Europe (Ireland), Alamat IP elastis `Y.Y.Y.Y`

Berikan semua catatan latensi nama domain yang sama, misalnya, `www-lbr.example.com` dan jenis yang sama, A.

Setelah Anda selesai membuat catatan latensi, Route 53 akan terus merutekan lalu lintas menggunakan catatan yang Anda perbarui di Langkah 2.

Anda dapat menggunakan `www-lbr.example.com` untuk pengujian validasi, misalnya, untuk memastikan bahwa setiap titik akhir dapat menerima permintaan.

4. Sekarang mari tambahkan catatan `www-lbr.example.com` latensi ke dalam catatan `www.example.com` tertimbang dan mulai merutekan lalu lintas terbatas ke instans Amazon

yang sesuai. EC2 Ini berarti bahwa EC2 instans Amazon di wilayah Timur AS (Ohio) akan mendapatkan lalu lintas dari kedua catatan tertimbang.

Buat catatan alias tertimbang lainnya untuk `www.example.com`:

- Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), pilih Alias to another record in this hosted zone (Alias ke catatan lain di zona yang di-hosting ini), dan tentukan `www-lbr.example.com`.
- Untuk Bobot, tentukan 1.

Ketika Anda selesai dan perubahan Anda disinkronkan ke server Route 53, Route 53 akan mulai merutekan sebagian kecil lalu lintas Anda (1/101) ke EC2 instans Amazon yang Anda buat catatan latensi di Langkah 3.

5. Saat Anda mengembangkan keyakinan bahwa titik akhir Anda diskalakan secara memadai untuk lalu lintas masuk, sesuaikan bobotnya. Misalnya, jika Anda ingin 10% dari permintaan Anda didasarkan pada perutean berbasis latensi, ubah bobot masing-masing menjadi 90 dan 10.

Untuk informasi lebih lanjut tentang membuat catatan latensi, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#).

Menambahkan Wilayah lain untuk perutean berbasis latensi Anda di Amazon Route 53

Jika Anda menggunakan perutean berbasis latensi dan ingin menambahkan instans di wilayah baru, Anda dapat mengalihkan lalu lintas ke wilayah baru secara bertahap dengan cara yang sama seperti Anda secara bertahap mengalihkan lalu lintas ke perutean berbasis latensi di [Transisi ke latensi berbasis perutean di Amazon Route 53](#).

Misalnya, Anda menggunakan perutean berbasis latensi untuk mengarahkan lalu lintas `www.example.com`, dan Anda ingin menambahkan EC2 instance Amazon di Asia Pasifik (Tokyo) ke instans Anda di AS Timur (Ohio), AS Barat (California N.), dan Eropa (Irlandia). Contoh prosedur berikut menjelaskan salah satu cara yang Anda dapat menambahkan instans di wilayah lain.

Untuk contoh ini, zona yang di-hosting Amazon Route 53 untuk `example.com` sudah memiliki catatan alias tertimbang untuk `www.example.com` yang merutekan lalu lintas ke catatan berbasis latensi untuk `www-lbr.example.com`:

- US East (Ohio), Alamat IP Elastis W.W.W.W
- US West (N. California), Alamat IP Elastis X.X.X.X
- Europe (Ireland), Alamat IP elastisY.Y.Y.Y

Catatan alias tertimbang memiliki berat 100. Setelah Anda beralih ke perutean berbasis latensi, asumsikan bahwa Anda menghapus catatan berbobot lain yang Anda gunakan untuk transisi.

Untuk menambahkan Wilayah lain ke perutean berbasis latensi Anda di Route 53

1. Buat empat rekaman berbasis latensi baru yang menyertakan tiga region asli serta wilayah baru tempat Anda ingin mulai merutekan lalu lintas.
 - US East (Ohio), Alamat IP Elastis W.W.W.W
 - US West (N. California), Alamat IP Elastis X.X.X.X
 - Europe (Ireland), Alamat IP elastisY.Y.Y.Y
 - Asia Pacific (Tokyo), alamat IP Elastis Z.Z.Z.Z

Berikan semua catatan latensi nama domain baru yang sama, misalnya, `www-lbr-2012-04-30.example.com`, dan jenis yang sama, A.

Setelah selesai membuat catatan latensi, Route 53 akan terus merutekan lalu lintas menggunakan alias tertimbang record (`www.example.com`) dan catatan latensi () asli. `www-lbr.example.com`

Anda dapat menggunakan catatan `www-lbr-2012-04-30.example.com` untuk pengujian validasi, misalnya, untuk memastikan bahwa setiap titik akhir dapat menerima permintaan.

2. Buat catatan alias tertimbang untuk catatan latensi baru:
 - Untuk nama domain, tentukan nama untuk catatan alias tertimbang yang ada, `www.example.com`.
 - Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), pilih Alias to another record in this hosted zone (Alias ke catatan lain di zona yang di-hosting ini), dan tentukan `www-lbr-2012-04-30.example.com`.
 - Untuk Bobot, tentukan 1.

Ketika Anda selesai, Route 53 akan mulai merutekan sebagian kecil dari lalu lintas Anda (1/101) ke EC2 instans Amazon yang Anda buat catatan `www-lbr-2012-04-30.example.com` latensi di Langkah 1. Sisa lalu lintas akan terus dialihkan ke catatan `www-lbr.example.com` latensi, yang tidak termasuk EC2 contoh Amazon di wilayah Asia Pasifik (Tokyo).

3. Saat Anda mengembangkan keyakinan bahwa titik akhir Anda diskalakan secara memadai untuk lalu lintas masuk, sesuaikan bobotnya. Misalnya, jika Anda ingin 10% permintaan Anda diarahkan ke catatan latensi yang mencakup wilayah Tokyo, ubah bobot untuk `www-lbr.example.com` dari 100 hingga 90 dan berat untuk `www-lbr-2012-04-30.example.com` dari 1 sampai 10.

Untuk informasi selengkapnya tentang cara membuat catatan, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#).

Menggunakan latensi dan catatan tertimbang di Amazon Route 53 untuk merutekan lalu lintas ke EC2 beberapa instans Amazon di suatu Wilayah

Jika aplikasi Anda berjalan di EC2 instans Amazon di dua atau lebih EC2 wilayah Amazon, dan jika Anda memiliki lebih dari satu EC2 instans Amazon di satu atau beberapa wilayah, Anda dapat menggunakan perutean berbasis latensi untuk merutekan lalu lintas ke wilayah yang benar dan kemudian menggunakan catatan tertimbang untuk merutekan lalu lintas ke instans dalam wilayah berdasarkan bobot yang Anda tentukan.

Misalnya, Anda memiliki tiga EC2 instans Amazon dengan alamat IP Elastic di wilayah AS Timur (Ohio) dan Anda ingin mendistribusikan permintaan di ketiganya IPs secara merata untuk pengguna yang wilayah yang sesuai dengan US East (Ohio). Hanya satu EC2 contoh Amazon yang cukup di wilayah lain, meskipun Anda dapat menerapkan teknik yang sama ke banyak wilayah sekaligus.

Untuk menggunakan latensi dan catatan tertimbang di Amazon Route 53 untuk merutekan lalu lintas ke EC2 beberapa instans Amazon di suatu wilayah

1. Buat grup catatan tertimbang untuk EC2 instans Amazon di wilayah tersebut. Perhatikan hal berikut:

- Berikan setiap catatan tertimbang nilai yang sama untuk Nama catatan (misalnya, `us-east.example.com`) dan Tipe catatan.
- Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), pilih IP address or another value depending on the record type (Alamat IP atau nilai lain tergantung jenis catatan), dan menentukan nilai dari salah satu alamat IP elastis.
- Jika Anda ingin menimbang EC2 instans Amazon secara merata, tentukan nilai yang sama untuk Berat.
- Tentukan nilai unik untuk Set ID untuk setiap catatan.

Untuk informasi selengkapnya tentang nilai rekaman tertimbang, lihat [Perutean tertimbang](#)

2. Jika Anda memiliki beberapa EC2 instans Amazon di wilayah lain, ulangi Langkah 1 untuk wilayah lain. Tentukan nilai yang berbeda untuk Nama di setiap daerah.
3. Untuk setiap wilayah di mana Anda memiliki beberapa EC2 instans Amazon (misalnya, US East (Ohio)), buat catatan alias latensi. Untuk Value/Route traffic to (Menilai/Merutekan lalu lintas), pilih Alias to another record in this hosted zone (Alias ke catatan lain di zona yang di-hosting ini), dan tentukan nilai bidang Record name (Catatan nama) (misalnya, `us-east.example.com`) yang Anda tetapkan ke catatan tertimbang di wilayah tersebut.
4. Untuk setiap wilayah di mana Anda memiliki satu EC2 instans Amazon, buat catatan latensi. Untuk Catatan nama, tentukan nilai yang sama yang Anda tentukan untuk catatan alias latensi yang Anda buat di langkah 3. Untuk lalu lintas Nilai/Rute ke, pilih alamat IP atau nilai lain tergantung pada jenis rekaman, dan tentukan alamat IP Elastis dari EC2 instans Amazon di Wilayah tersebut.

Untuk informasi selengkapnya tentang menambahkan catatan alias ke EC2 instans Amazon, lihat [Merutekan lalu lintas ke instans Amazon EC2](#)

Untuk informasi selengkapnya tentang cara membuat catatan, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#).

Mengelola lebih 100 catatan tertimbang di Amazon Route 53

Di Amazon Route 53 Anda dapat mengonfigurasi catatan tertimbang. Untuk nama dan jenis tertentu (misalnya, `www.example.com`, tipe A), Anda dapat mengkonfigurasi hingga 100 tanggapan alternatif, masing-masing dengan beratnya sendiri. Ketika menanggapi pertanyaan untuk

`www.example.com`, server DNS Route 53 memilih respons acak tertimbang untuk kembali ke DNS resolver. Nilai catatan tertimbang yang memiliki bobot 2 dihasilkan, rata-rata, dua kali lebih sering dari nilai catatan tertimbang yang memiliki bobot 1.

Jika Anda perlu mengarahkan lalu lintas ke lebih dari 100 titik akhir, salah satu cara untuk mencapainya adalah dengan menggunakan pohon catatan alias berbobot dan catatan berbobot. Misalnya, "level" pertama dari pohon mungkin berisi hingga 100 catatan alias berbobot, yang masing-masing dapat, pada gilirannya, menunjuk hingga 100 catatan berbobot. Route 53 memungkinkan hingga tiga tingkat rekursi, memungkinkan Anda untuk mengelola hingga 1.000.000 titik akhir berbobot unik.

Pohon dua tingkat sederhana mungkin terlihat seperti ini:

Catatan alias tertimbang

- Alias `www.example.com` untuk `www-a.example.com` dengan bobot 1
- Alias `www.example.com` untuk `www-b.example.com` dengan bobot 1

Catatan tertimbang

- `www-a.example.com`, tipe A, nilai 192.0.2.1, bobot 1
- `www-a.example.com`, tipe A, nilai 192.0.2.2, bobot 1
- `www-b.example.com`, tipe A, nilai 192.0.2.3, bobot 1
- `www-b.example.com`, tipe A, nilai 192.0.2.4, bobot 1

Untuk informasi selengkapnya tentang cara membuat catatan, lihat [Bekerja dengan catatan](#).

Menimbang jawaban multicatatan yang toleran terhadap kesalahan di Amazon Route 53

Note

Catatan yang menggunakan kebijakan perutean jawaban multinilai berperilaku dengan cara yang sama seperti konfigurasi yang didokumentasikan dalam tutorial ini. Perbedaan utamanya adalah konfigurasi tutorial memungkinkan Anda menentukan bobot, yang

dapat berguna ketika titik akhir Anda memiliki kapasitas yang berbeda. Untuk informasi selengkapnya, lihat [Perutean jawaban multিনিলাই](#).

Catatan tertimbang Amazon Route 53 hanya dapat dikaitkan dengan satu catatan, yang berarti kombinasi dari satu nama (misalnya, `example.com`) dan satu jenis catatan (misalnya, A). Namun, ini sering kali diinginkan untuk menimbang respons DNS yang berisi banyak catatan.

Misalnya, Anda mungkin memiliki delapan EC2 instans Amazon atau titik akhir IP Elastis untuk suatu layanan. Jika klien layanan tersebut mendukung koneksi mencoba lagi (seperti yang dilakukan semua peramban umum), maka memberikan beberapa alamat IP dalam respons DNS memberi klien tersebut titik akhir alternatif jika terjadi kegagalan titik akhir tertentu. Anda bahkan dapat melindungi dari kegagalan zona ketersediaan jika Anda mengonfigurasi respons untuk berisi campuran IPs host di dua atau lebih zona ketersediaan.

Jawaban multicatatan juga berguna ketika sejumlah besar klien (misalnya, aplikasi web seluler) berbagi satu kumpulan kecil cache DNS. Dalam hal ini, jawaban multicatatan memungkinkan klien untuk mengarahkan permintaan ke beberapa titik akhir bahkan jika mereka menerima respons DNS umum dari cache bersama.

Jenis jawaban multicatatan berbobot ini dapat dicapai dengan menggunakan kombinasi catatan dan catatan alias berbobot. Anda dapat mengelompokkan delapan titik akhir menjadi dua kumpulan catatan berbeda yang masing-masing berisi empat alamat IP:

`endpoint-a.example.com`, ketik A, dengan nilai berikut:

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, ketik A, dengan nilai berikut:

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

Anda kemudian dapat membuat catatan alias tertimbang yang menunjuk ke setiap grup:

- Alias `www.example.com` untuk `endpoint-a.example.com`, tipe A, bobot 1
- Alias `www.example.com` untuk `endpoint-b.example.com`, tipe A, bobot 1

Untuk informasi selengkapnya tentang cara membuat catatan, lihat [Bekerja dengan catatan](#).

Praktik terbaik untuk Amazon Route 53

Bagian ini memberikan praktik terbaik untuk berbagai komponen Amazon Route 53, termasuk:

1. Praktik terbaik DNS:

- Memahami trade-off antara nilai time to live (TTL) dan daya tanggap versus keandalan.
- Gunakan catatan alias alih-alih catatan CNAME bila memungkinkan untuk meningkatkan kinerja dan penghematan biaya.
- Konfigurasi kebijakan perutean default untuk memastikan semua klien menerima respons.
- Memanfaatkan routing berbasis latensi untuk meminimalkan latensi aplikasi dan routing untuk stabilitas dan geolocation/geoproximity prediktabilitas.
- Verifikasi propagasi perubahan menggunakan GetChange API untuk alur kerja otomatis.
- Delegasikan subdomain dari zona induk untuk perutean yang konsisten.
- Hindari respons tunggal yang besar dengan menggunakan routing jawaban multivalue.

2. Praktik terbaik penyelesaian:

- Cegah perutean loop dengan menghindari mengaitkan VPC yang sama dengan aturan Resolver dan titik akhir masuknya.
- Menerapkan aturan grup keamanan untuk mengurangi overhead pelacakan koneksi dan memaksimalkan throughput kueri.
- Konfigurasi titik akhir masuk dengan alamat IP di beberapa Availability Zone untuk redundansi.
- Waspada potensi serangan berjalan zona DNS dan hubungi AWS Support jika titik akhir Anda mengalami pelambatan.

3. Health Check Best Practices:

- Ikuti rekomendasi untuk mengoptimalkan pemeriksaan kesehatan Amazon Route 53 untuk memastikan pemantauan sumber daya Anda yang andal

Dengan mengikuti praktik terbaik ini, Anda dapat mengoptimalkan kinerja, keandalan, dan keamanan infrastruktur DNS Anda, memastikan perutean lalu lintas yang efisien dan efektif ke aplikasi dan layanan Anda

Topik

- [Praktik terbaik untuk Amazon Route 53 DNS](#)

- [Praktik terbaik untuk VPC Resolver](#)
- [Praktik terbaik untuk pemeriksaan kondisi Amazon Route 53](#)

Praktik terbaik untuk Amazon Route 53 DNS

Ikuti praktik terbaik ini untuk mendapatkan hasil terbaik saat menggunakan layanan DNS Amazon Route 53.

Gunakan fungsi bidang data untuk failover DNS dan pemulihan aplikasi

Pesawat data untuk Route 53, termasuk pemeriksaan kesehatan, dan kontrol perutean Amazon Application Recovery Controller (ARC) didistribusikan secara global, dan dirancang untuk ketersediaan dan fungsionalitas 100%, bahkan selama kejadian parah. Mereka berintegrasi satu sama lain dan tidak bergantung pada fungsionalitas bidang kontrol. Sementara pesawat kontrol untuk layanan ini, termasuk konsol mereka, umumnya sangat andal, mereka dirancang dengan cara yang lebih terpusat dan memprioritaskan daya tahan dan konsistensi daripada ketersediaan tinggi. Untuk skenario seperti failover selama pemulihan bencana, kami menyarankan Anda menggunakan fitur seperti pemeriksaan kesehatan Route 53 dan kontrol perutean ARC yang mengandalkan fungsionalitas pesawat data untuk memperbarui DNS. Untuk informasi selengkapnya, lihat [Konsep bidang kontrol dan data](#) dan [Blog: Membuat Mekanisme Pemulihan Bencana Menggunakan Amazon Route 53](#).

Memilih nilai TTL untuk catatan DNS

DNS TTL adalah nilai numerik (dalam detik) yang digunakan oleh penyelesai DNS untuk memutuskan berapa lama rekaman dapat di-cache tanpa membuat kueri lain ke Route 53. Semua catatan DNS harus memiliki TTL yang ditentukan untuk mereka. Rentang yang disarankan untuk nilai TTL adalah 60 hingga 172.800 detik.

Pilihan TTL adalah trade-off antara latensi dan keandalan, dan responsif terhadap perubahan. Dengan catatan yang lebih pendek TTLs, penyelesai DNS melihat pembaruan ke rekaman lebih cepat karena mereka harus lebih sering melakukan kueri. Ini meningkatkan volume kueri (dan biaya). Saat Anda memperpanjang TTL, penyelesai DNS menjawab pertanyaan dari cache lebih sering, yang biasanya lebih cepat, lebih murah, dan dalam beberapa situasi, lebih dapat diandalkan, karena menghindari kueri di internet. Tidak ada nilai yang benar, tetapi ada baiknya untuk memikirkan apakah daya tanggap atau keandalan lebih penting bagi Anda.

Hal-hal yang perlu dipertimbangkan ketika Anda menetapkan nilai TTL meliputi:

- Tetapkan catatan DNS TTLs untuk jangka waktu yang Anda mampu menunggu perubahan diterapkan. Hal ini terutama berlaku pada delegasi (set catatan NS), atau catatan lain yang jarang berubah, misalnya catatan MX. Untuk catatan ini, lebih lama TTLs direkomendasikan. Nilai antara satu jam (3600-an) dan satu hari (86.400 detik) adalah pilihan umum.
- Untuk catatan yang perlu diubah sebagai bagian dari mekanisme failover cepat (terutama catatan yang diperiksa kesehatan), yang lebih rendah TTLs adalah tepat. Mengatur TTL 60 atau 120 detik adalah pilihan umum untuk skenario ini.
- Ketika Anda ingin membuat perubahan pada entri DNS kritis, kami sarankan Anda untuk sementara mempersingkat entri DNS. TTLs Kemudian Anda dapat melakukan perubahan, mengamati, dan mengembalikan dengan cepat jika perlu. Setelah perubahan diselesaikan dan berfungsi seperti yang diharapkan, Anda dapat meningkatkan TTL.

Untuk mengetahui informasi selengkapnya, lihat [TTL \(detik\)](#).

Catatan CNAME

Catatan DNS CNAME adalah cara untuk mengarahkan satu nama domain ke yang lain. Jika penyelesai DNS menyelesaikan domain-1.example.com dan menemukan CNAME menunjuk ke, penyelesai DNS harus melanjutkan untuk menyelesaikan sebelum dapat merespons. domain-2.example.com domain-2.example.com Catatan ini berguna dalam banyak situasi, misalnya, untuk memastikan konsistensi ketika situs web memiliki lebih dari satu nama domain.

Namun, penyelesai DNS harus membuat lebih banyak pertanyaan untuk dijawab CNAMEs, yang meningkatkan latensi dan biaya. Jika memungkinkan, alternatif yang lebih cepat dan lebih murah adalah dengan menggunakan catatan alias Route 53. Catatan alias memungkinkan Route 53 merespons dengan jawaban langsung untuk AWS sumber daya (misalnya, penyeimbang beban) dan untuk domain lain dalam zona host yang sama.

Untuk informasi selengkapnya, lihat [Merutekan lalu lintas internet ke sumber daya Anda AWS](#).

Perutean DNS tingkat lanjut

- Saat menggunakan geolokasi, geoproximity, atau perutean berbasis latensi, selalu tetapkan default, kecuali jika Anda ingin beberapa klien tidak menerima tanggapan jawaban.
- Untuk meminimalkan latensi aplikasi, gunakan perutean berbasis latensi. Jenis data routing ini dapat sering berubah.
- Untuk memberikan stabilitas dan prediktabilitas perutean, gunakan perutean geolokasi atau geoproximity.

Lihat informasi selengkapnya di [Perutean geolokasi](#), [Perutean geoproksimitas](#), dan [Perutean berbasis latensi](#).

Perambatan perubahan DNS

Saat Anda membuat atau memperbarui rekaman atau zona yang dihosting dengan menggunakan konsol atau API Route 53, perubahan akan tercermin di internet. Ini disebut propagasi perubahan. Sementara propagasi biasanya memakan waktu kurang dari satu menit secara global, kadang-kadang ada penundaan, misalnya, karena masalah sinkronisasi ke satu lokasi, atau dalam kasus yang jarang terjadi, masalah dalam bidang kontrol pusat. Jika Anda sedang membangun alur kerja penyediaan otomatis, dan penting untuk menunggu propagasi perubahan selesai sebelum Anda melanjutkan dengan langkah alur kerja berikutnya, gunakan [GetChangeAPI](#) untuk memverifikasi bahwa perubahan DNS Anda telah berlaku (). Status =INSYNC

Delegasi DNS

Saat Anda mendelegasikan beberapa level subdomain di DNS, penting untuk selalu mendelegasikan dari zona induk. Misalnya, jika Anda mendelegasikan `www.dept.example.com`, Anda harus melakukannya dari `dept.example.com` zona, bukan dari `example.com` zona. Delegasi dari kakek-nenek ke zona anak mungkin tidak berfungsi sama sekali atau hanya bekerja secara tidak konsisten. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas untuk subdomain](#).

Ukuran respons DNS

Hindari membuat respons tunggal yang besar. Jika respons lebih besar dari 512 byte, banyak penyelesaian DNS harus mencoba lagi melalui TCP alih-alih UDP, yang dapat mengurangi keandalan dan menyebabkan respons yang lebih lambat. Sebaiknya gunakan routing jawaban multivalue, yang memilih delapan alamat IP acak yang sehat untuk menjaga respons dalam batas 512 byte.

Untuk informasi selengkapnya, lihat [Perutean jawaban multinilai](#) dan [Server Uji Ukuran Balas DNS](#).

Praktik terbaik untuk VPC Resolver

Bagian ini memberikan praktik terbaik untuk mengoptimalkan Amazon Route 53 VPC Resolver, yang mencakup topik-topik berikut:

1. Menghindari Konfigurasi Loop dengan Titik Akhir Resolver:

- Cegah perutean loop dengan memastikan bahwa VPC yang sama tidak terkait dengan aturan Resolver dan titik akhir masuknya.
- Gunakan AWS RAM untuk berbagi VPCs di seluruh akun sambil mempertahankan konfigurasi perutean yang tepat.

Untuk informasi selengkapnya, lihat [Hindari konfigurasi loop dengan titik akhir Resolver](#)

2. Titik akhir Resolver Penskalaan:

- Menerapkan aturan grup keamanan yang mengizinkan lalu lintas berdasarkan status koneksi untuk mengurangi overhead pelacakan koneksi
- Ikuti aturan grup keamanan yang disarankan untuk titik akhir Resolver masuk dan keluar untuk memaksimalkan throughput kueri.
- Pantau alamat IP unik dan kombinasi port yang menghasilkan lalu lintas DNS untuk menghindari keterbatasan kapasitas.

Untuk informasi selengkapnya, lihat [Penskalaan titik akhir penyelesai](#)

3. Ketersediaan tinggi untuk titik akhir Resolver:

- Buat titik akhir masuk dengan alamat IP di setidaknya dua Availability Zone untuk redundansi.
- Menyediakan antarmuka jaringan tambahan untuk memastikan ketersediaan selama pemeliharaan atau lonjakan lalu lintas

Untuk informasi selengkapnya, lihat [Ketersediaan tinggi untuk titik akhir Resolver](#)

4. Mencegah serangan berjalan zona DNS:

- Waspada potensi serangan berjalan zona DNS, di mana penyerang mencoba mengambil semua konten dari zona DNS yang ditandatangani DNSSEC.
- Jika titik akhir Anda mengalami pelambatan karena dicurigai berjalan di zona, hubungi AWS Support untuk bantuan.

Untuk informasi selengkapnya, lihat [Zona DNS berjalan](#)

Dengan mengikuti praktik terbaik ini, Anda dapat mengoptimalkan kinerja, skalabilitas, dan keamanan penerapan Resolver VPC Anda, memastikan resolusi DNS yang andal dan efisien untuk aplikasi dan sumber daya Anda.

Hindari konfigurasi loop dengan titik akhir Resolver

Jangan mengaitkan VPC yang sama ke aturan Resolver dan titik akhir masuknya (apakah itu target langsung titik akhir, atau melalui server DNS on-premise). Ketika titik akhir keluar dalam aturan Resolver menunjuk ke titik akhir masuk yang berbagi VPC dengan aturan, hal ini dapat menyebabkan loop di mana kueri terus diteruskan di antara titik akhir masuk dan keluar.

Aturan penerusan masih dapat dikaitkan dengan yang lain VPCs yang dibagikan dengan akun lain dengan menggunakan AWS Resource Access Manager (AWS RAM). Zona yang di-hosting secara privat yang terkait dengan hub, atau VPC sentral, masih akan menyelesaikan dari kueri ke titik akhir masuk, karena aturan penyelesai penerusan tidak mengubah resolusi ini.

Penskalaan titik akhir penyelesai

Grup keamanan titik akhir penyelesai menggunakan pelacakan koneksi untuk mengumpulkan informasi tentang lalu lintas ke dan dari titik akhir. Setiap antarmuka titik akhir memiliki jumlah maksimum koneksi yang dapat dilacak, dan volume kueri DNS yang tinggi dapat melebihi koneksi serta menyebabkan throttling dan kehilangan kueri. Pelacakan koneksi AWS adalah perilaku default untuk memantau keadaan lalu lintas yang mengalir melalui grup keamanan (SGs). Menggunakan pelacakan koneksi SGs akan mengurangi throughput lalu lintas, namun, Anda dapat menerapkan koneksi yang tidak dilacak untuk mengurangi overhead dan meningkatkan kinerja. Untuk informasi selengkapnya lihat Koneksi [yang tidak dilacak](#).

Jika pelacakan koneksi diberlakukan baik dengan menggunakan aturan grup keamanan yang membatasi atau kueri dirutekan melalui Network Load Balancer (lihat [Koneksi yang dilacak secara otomatis](#)), kueri maksimum keseluruhan per detik per alamat IP untuk titik akhir bisa serendah 1500.

Rekomendasi aturan Grup Keamanan masuk dan keluar untuk titik akhir Resolver masuk

Aturan masuk

Jenis protokol	Nomor port	Sumber IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

Aturan jalan keluar

Jenis protokol	Nomor port	IP Tujuan

TCP	Semua	0.0.0.0/0
UDP	Semua	0.0.0.0/0

Rekomendasi aturan grup keamanan masuk dan keluar untuk titik akhir Resolver keluar

Aturan masuk

Jenis protokol	Nomor port	Sumber IP
TCP	Semua	0.0.0.0/0
UDP	Semua	0.0.0.0/0

Aturan jalan keluar

Jenis protokol	Nomor port	IP Tujuan
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

Note

Persyaratan port grup keamanan:

- Endpoint inbound memerlukan aturan ingress yang memungkinkan TCP dan UDP pada port 53 untuk menerima kueri DNS dari jaringan Anda. Aturan keluar dapat mengizinkan semua port karena titik akhir mungkin perlu menanggapi kueri dari berbagai port sumber.
- Titik akhir keluar memerlukan aturan keluar yang memungkinkan akses TCP dan UDP ke port yang Anda gunakan untuk kueri DNS di jaringan Anda. Port 53 ditunjukkan pada contoh di atas karena ini adalah port DNS yang paling umum, tetapi jaringan Anda mungkin menggunakan port yang berbeda. Aturan Ingress dapat memungkinkan semua port untuk mengakomodasi respons dari server DNS Anda.

Titik akhir Inbound Resolver

Untuk klien yang menggunakan titik akhir Resolver masuk, kapasitas antarmuka jaringan elastis akan terpengaruh jika Anda memiliki lebih dari 40.000 alamat IP unik dan port kombinasi yang menghasilkan lalu lintas DNS.

Ketersediaan tinggi untuk titik akhir Resolver

Saat Anda membuat titik akhir masuk VPC Resolver, Route 53 mengharuskan Anda membuat setidaknya dua alamat IP yang akan diteruskan kueri oleh resolver DNS di jaringan Anda. Anda juga harus menentukan alamat IP di setidaknya dua Availability Zone untuk redundansi.

Jika memerlukan lebih dari satu titik akhir antarmuka jaringan elastis agar tersedia setiap saat, kami sarankan Anda menambahkan setidaknya satu antarmuka jaringan melebihi kebutuhan, untuk memastikan Anda memiliki kapasitas tambahan yang tersedia untuk menangani kemungkinan lonjakan lalu lintas. Antarmuka jaringan tambahan juga memastikan ketersediaan selama operasi layanan seperti pemeliharaan atau peningkatan.

Untuk informasi lebih lanjut, lihat artikel blog terperinci ini: [Cara mencapai ketersediaan tinggi DNS dengan titik akhir Resolver](#) dan [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#)

Zona DNS berjalan

Serangan zona DNS berjalan mencoba untuk mendapatkan semua konten dari zona DNS yang ditandatangani DNSSEC. Jika tim VPC Resolver mendeteksi pola lalu lintas yang cocok dengan yang dihasilkan saat zona DNS berjalan di titik akhir Anda, tim layanan akan membatasi lalu lintas di titik akhir Anda. Sebagai konsekuensinya, Anda mungkin melihat persentase tinggi pada batas waktu kueri DNS.

Jika Anda mengamati pengurangan kapasitas pada titik akhir Anda dan yakin bahwa titik akhir telah dibatasi secara keliru, pergilah ke <https://console.aws.amazon.com/support/> rumah#/ untuk membuat kasus dukungan.

Praktik terbaik untuk pemeriksaan kondisi Amazon Route 53

Konfigurasi pemeriksaan kesehatan yang efektif sangat penting untuk menjaga infrastruktur yang sangat tersedia dan tangguh. Berikut adalah beberapa praktik terbaik yang perlu dipertimbangkan saat menyiapkan dan mengelola pemeriksaan kesehatan Amazon Route 53:

1. Gunakan alamat IP elastis untuk titik akhir pemeriksaan kesehatan:

- Gunakan alamat IP elastis untuk titik akhir pemeriksaan kesehatan Anda untuk memastikan pemantauan yang konsisten.
- Jika Anda tidak lagi menggunakan EC2 instans Amazon, ingatlah untuk menghapus pemeriksaan kesehatan terkait untuk menghindari potensi risiko keamanan atau kompromi data.

Untuk informasi lebih lanjut, lihat [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#).

2. Konfigurasi interval pemeriksaan kesehatan yang sesuai:

- Tetapkan interval pemeriksaan kesehatan berdasarkan persyaratan aplikasi Anda dan kekritisannya sumber daya yang dipantau.
- Interval yang lebih pendek memberikan deteksi kegagalan yang lebih cepat tetapi dapat meningkatkan biaya Route 53 dan memuat sumber daya Anda.
- Interval yang lebih lama mengurangi biaya dan beban sumber daya tetapi dapat menunda deteksi kegagalan.

Untuk informasi lebih lanjut, lihat [Konfigurasi lanjutan \("Pantau Titik Akhir" saja\)](#).

3. Menerapkan pemberitahuan alarm:

- Konfigurasi Amazon CloudWatch alarms untuk menerima pemberitahuan saat pemeriksaan kesehatan gagal atau pulih.
- Tetapkan ambang alarm yang sesuai berdasarkan persyaratan aplikasi Anda dan perilaku sumber daya yang diharapkan.
- Integrasikan notifikasi dengan proses pemantauan dan respons insiden Anda.

Untuk informasi lebih lanjut, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

4. Memanfaatkan pemeriksaan kesehatan Daerah secara strategis:

- Pilih pemeriksaan kesehatan Wilayah berdasarkan distribusi geografis pengguna dan sumber daya Anda.
- Pertimbangkan untuk menggunakan beberapa wilayah pemeriksaan kesehatan untuk sumber daya penting guna meningkatkan keandalan dan mengurangi dampak pemadaman regional.

5. Pantau log dan metrik pemeriksaan kesehatan:

- Tinjau log dan CloudWatch metrik pemeriksaan kesehatan Route 53 secara teratur untuk mengidentifikasi potensi masalah atau kemacetan kinerja
- Menganalisis alasan kegagalan pemeriksaan kesehatan dan mengambil tindakan yang tepat untuk menyelesaikan masalah yang mendasarinya.

6. Menerapkan Strategi Failover dan Failback:

- Manfaatkan kebijakan routing failover Route 53 untuk secara otomatis merutekan lalu lintas ke sumber daya yang sehat jika terjadi kegagalan.
- Merencanakan dan menguji proses failover dan failback untuk memastikan transisi yang mulus selama pemadaman dan pemulihan.

Untuk informasi lebih lanjut, lihat [Mengonfigurasi failover DNS](#).

7. Tinjau dan Perbarui Pemeriksaan Kesehatan Secara Teratur:

- Perbarui titik akhir pemeriksaan kesehatan, interval, dan ambang alarm sesuai kebutuhan untuk mempertahankan pemantauan dan kinerja yang optimal.

Dengan mengikuti praktik terbaik ini, Anda dapat secara efektif memanfaatkan pemeriksaan kesehatan Amazon Route 53 untuk memantau kesehatan dan ketersediaan sumber daya kami, memastikan infrastruktur yang andal dan berkinerja tinggi untuk aplikasi dan layanan Anda.

Kuota

Permintaan API Amazon Route 53 dan entitas tunduk pada kuota berikut (sebelumnya disebut sebagai "batas").

Topik

- [Menggunakan Service Quotas untuk melihat dan mengelola kuota](#)
- [Kuota pada entitas](#)
- [Maksimum pada permintaan API](#)

Menggunakan Service Quotas untuk melihat dan mengelola kuota

Anda dapat menggunakan layanan Service Quotas untuk melihat kuota dan meminta peningkatan kuota bagi beragam layanan AWS. Untuk informasi lebih lanjut, lihat [Panduan Pengguna Service Quotas](#). (Saat ini Anda dapat menggunakan Service Quotas untuk melihat dan mengelola domain, kuota Route 53, dan Route 53 VPC Resolver.)

Note

Untuk melihat kuota dan meminta lebih banyak kuota Route 53, Anda harus mengubah Wilayah menjadi US East (N. Virginia). Untuk melihat kuota dan meminta kuota yang lebih tinggi untuk VPC Resolver, ubah ke Region yang berlaku.

Kuota pada entitas

Entitas Amazon Route 53 tunduk pada kuota berikut.

Untuk informasi tentang mendapatkan kuota saat ini (sebelumnya disebut sebagai "batas"), lihat tindakan Route 53 berikut:

- [GetAccountLimit](#)— Mendapat kuota pada pemeriksaan kesehatan, zona yang dihosting, set delegasi yang dapat digunakan kembali, kebijakan arus lalu lintas, dan catatan kebijakan arus lalu lintas
- [GetHostedZoneLimit](#)— Mendapat kuota pada catatan di zona yang dihosting dan di Amazon VPCs yang dapat Anda kaitkan dengan zona host pribadi

- [GetReusableDelegationSetLimit](#)— Mendapatkan kuota pada jumlah zona yang dihosting yang dapat Anda kaitkan dengan kumpulan delegasi yang dapat digunakan kembali

Topik

- [Kuota pada domain](#)
- [Kuotas pada zona yang di-hosting](#)
- [Kuota pada catatan](#)
- [Kuota pada Route 53 VPC Resolver](#)
- [Kuota pada pemeriksaan kondisi](#)
- [Kuota pada konfigurasi log kueri](#)
- [Kuota tentang kebijakan alur lalu lintas dan catatan kebijakan](#)
- [Kuota pada set delegasi dapat digunakan kembali](#)
- [Kuota pada Profil Route 53](#)

Kuota pada domain

Entitas	Kuota
Domain	20* per akun AWS Meminta kuota yang lebih tinggi.

*Batasnya adalah 20 untuk pelanggan baru per Maret 2021.

Jika Anda sudah memiliki akun dan batas default saat ini adalah 50, batas akan tetap berjumlah 50.

Kuotas pada zona yang di-hosting

Entitas	Kuota
Zona yang di-hosting	Kuota awal 500 per AWS akun, tetapi Anda dapat meminta kuota yang lebih tinggi sesuai kebutuhan.

Entitas	Kuota
	Meminta kuota yang lebih tinggi.
Zona yang di-hosting yang dapat menggunakan set delegasi yang dapat digunakan kembali yang sama	100 Meminta kuota yang lebih tinggi.
Amazon VPCs yang dapat Anda kaitkan dengan zona host pribadi per zona yang dihosting	300 Jika Anda menginginkan lebih dari 300 asosiasi, kami sarankan Anda menggunakan Route 53 Profiles. Untuk informasi selengkapnya, lihat Apa itu Profil Amazon Route 53? .
Zona yang di-hosting secara pribadi yang dapat Anda kaitkan dengan VPC	Tidak ada kuota*
Otorisasi yang dapat Anda buat sehingga Anda dapat mengaitkan VPCs yang dibuat oleh satu akun dengan zona host yang dibuat oleh akun lain	1000
Jumlah kunci penandatanganan kunci (KSK) yang dapat Anda buat per zona yang di-hosting	2

* Anda dapat mengaitkan VPC dengan salah satu atau semua zona host pribadi yang Anda kontrol melalui akun Anda AWS . Misalnya, Anda memiliki tiga AWS akun dan ketiganya memiliki kuota default 500 zona yang dihosting. Jika membuat 500 zona yang di-hosting secara privat untuk ketiga akun, Anda dapat mengaitkan VPC dengan 1.500 zona yang di-hosting secara privat.

Kuota pada catatan

Entitas	Kuota
Catatan	10.000 per zona yang di-hosting Meminta kuota yang lebih tinggi. Untuk kuota lebih dari 10.000 catatan di zona yang dihosting, dikenakan biaya tambahan. Untuk informasi selengkapnya, lihat Harga Amazon Route 53.
Rekaman dalam set rekor	400 per rekor yang ditetapkan
Geolokasi, latensi, jawaban multivalu e, tertimbang, dan catatan berbasis IP	100 catatan dengan nama dan jenis yang sama
Catatan geoproximity	30 catatan dengan nama dan jenis yang sama
Koleksi CIDR	5 per Akun AWS. Meminta kuota yang lebih tinggi.
Blok CIDR	1000 per koleksi CIDR. Meminta kuota yang lebih tinggi.

Kuota pada Route 53 VPC Resolver

Bagian ini mencakup semua kuota Route 53 VPC Resolver

Kuota pada Route 53 VPC Resolver

Gunakan prosedur berikut untuk meningkatkan kuota untuk Route 53 VPC Resolver.

Untuk meningkatkan kuota Resolver

1. Buka konsol Service Quotas di <https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas>.
2. Pergi ke wilayah yang ingin Anda tingkatkan batasnya.
3. Pilih nama Kuota Resolver VPC Route 53 yang ingin Anda tingkatkan.
4. Pilih Minta peningkatan kuota, masukkan nilai kuota, lalu pilih Minta.

Kuota pada titik akhir Route 53 VPC Resolver

Entitas	Kuota
Titik akhir per Wilayah AWS	4 per AWS akun Meminta kuota yang lebih tinggi.
Alamat IP per titik akhir	6 Meminta kuota yang lebih tinggi.
Alamat IP per aturan	6
Aturan per AWS Wilayah	1000 per AWS akun Meminta kuota yang lebih tinggi.
Asosiasi antara aturan dan VPCs per AWS Wilayah	2000 per AWS akun Meminta kuota yang lebih tinggi.
Kueri UDP per detik per alamat IP di titik akhir	10.000*

* Setiap alamat IP di titik akhir dapat memproses hingga 10.000 kueri DNS UDP per detik (QPS). Jumlah DNS QPS bervariasi menurut jenis kueri, ukuran respons, kesehatan server nama target, waktu respons kueri, latensi pulang pergi, dan protokol yang digunakan. Sebagai contoh, permintaan ke server nama target yang lambat merespons secara signifikan dapat mengurangi kapasitas antarmuka jaringan. Selain itu, untuk memastikan ketersediaan tinggi, Route 53 Resolver menghasilkan kueri keluar redundan untuk setiap permintaan DNS yang diterima. Akibatnya, QPS untuk setiap antarmuka jaringan keluar tidak akan cocok dengan QPS yang dikirim ke Route 53 VPC Resolver. Gunakan CloudWatch metrik untuk mengukur berapa banyak kueri yang dikirim ke setiap antarmuka jaringan. Untuk informasi selengkapnya, lihat [Metrik untuk alamat IP Route 53 VPC Resolver](#). Jika tingkat kueri maksimum melebihi 50% dari kapasitas untuk setiap antarmuka jaringan di titik akhir, Anda dapat menambahkan lebih banyak antarmuka jaringan untuk meningkatkan kapasitas titik akhir.

Koneksi yang dibuat melalui aplikasi seperti Network Load Balancer dan AWS Lambda (untuk daftar lengkap lihat [Koneksi yang dilacak secara otomatis](#)) dilacak secara otomatis, bahkan jika konfigurasi grup keamanan tidak memerlukan pelacakan.

Jika pelacakan koneksi diberlakukan baik dengan menggunakan aturan grup keamanan yang membatasi atau kueri dirutekan melalui Network Load Balancer, kueri maksimum keseluruhan per detik per alamat IP untuk titik akhir masuk bisa serendah 1500.

Kuota pada log kueri Route 53 VPC Resolver

Entitas	Kuota
Konfigurasi log kueri per Wilayah AWS	20 Meminta kuota yang lebih tinggi.
Konfigurasi log kueri pengaitan VPC per Wilayah AWS	100 * Meminta kuota yang lebih tinggi.
Konfigurasi log kueri Asosiasi VPC per akun per AWS Wilayah (termasuk kueri kueri kueri panjang yang dibagikan menggunakan	100 Meminta kuota yang lebih tinggi.

Entitas	Kuota
RAM) untuk akun tempat konfigurasi dibagikan.	

* Ini adalah batas Regional yang berlaku secara kumulatif di semua konfigurasi log kueri VPC Resolver dalam satu Wilayah. Membuat konfigurasi log kueri tambahan di Wilayah yang sama tidak memberikan kapasitas asosiasi VPC tambahan.

Kuota pada Resolver DNS Firewall

Entitas	Kuota
Jumlah grup aturan yang terkait dengan VPC untuk satu akun per Wilayah AWS	5
Jumlah domain DNS Firewall dalam satu file Amazon S3 untuk satu akun per Wilayah AWS	250.000 Meminta kuota yang lebih tinggi.
Jumlah grup aturan DNS Firewall untuk satu akun per Wilayah AWS	1.000 Meminta kuota yang lebih tinggi.
Jumlah aturan dalam grup aturan untuk satu akun per AWS Wilayah	100 Meminta kuota yang lebih tinggi.
Jumlah daftar domain untuk satu akun per AWS Wilayah	1000 Meminta kuota yang lebih tinggi.
Jumlah maksimum domain yang dapat Anda tentukan di semua daftar	100.000 Meminta kuota yang lebih tinggi.

Entitas	Kuota
domain untuk satu akun per Wilayah AWS	

Kuota pada Resolver di Outpost

Entitas	Kuota
Resolver pada batas instans Outpost	6 (dengan minimal 4 diperlukan)

Resolver pada jenis instans Outpost dan jumlah kueri DNS per detik setiap jenis instans dapat mengakomodasi:

Tipe instans	Kueri per detik
c5.large	Hingga 7.000
c5.xlarge	Hingga 12.000
c5.2xlarge	Hingga 24.000
c5.4xlarge	Hingga 56.000
c5d.large	Hingga 7.000
c5d.xlarge	Hingga 12.000
c5d.2xlarge	Hingga 24.000
c5d.4xlarge	Hingga 56.000
m5.large	Hingga 7.000

Tipe instans	Kueri per detik
m5.xlarge	Hingga 12.000
m5.2xlarge	Hingga 24.000
m5.4xlarge	Hingga 56.000
m5d.large	Hingga 7.000
m5d.xlarge	Hingga 12.000
m5d.2xlarge	Hingga 24.000
m5d.4xlarge	Hingga 56.000
r5.large	Hingga 7.000
r5.xlarge	Hingga 12.000
r5.2xlarge	Hingga 24.000
r5.4xlarge	Hingga 56.000
r5d.large	Hingga 7.000
r5d.xlarge	Hingga 12.000
r5d.2xlarge	Hingga 24.000

Tipe instans	Kueri per detik
r5d.4xlarge	Hingga 56.000

Resolver pada jenis instans titik akhir Outpost dan jumlah kueri DNS per detik setiap jenis instans dapat mengakomodasi:

Tipe instans	Kueri per detik
c5.large	Hingga 5.000
c5.xlarge	Hingga 10.000
c5.2xlarge	Hingga 18.000
c5.4xlarge	Hingga 30.000
c5d.large	Hingga 5.000
c5d.xlarge	Hingga 10.000
c5d.2xlarge	Hingga 18.000
c5d.4xlarge	Hingga 30.000
m5.large	Hingga 5.000
m5.xlarge	Hingga 10.000
m5.2xlarge	Hingga 18.000
m5.4xlarge	Hingga 30.000

Tipe instans	Kueri per detik
m5d.large	Hingga 5.000
m5d.xlarge	Hingga 10.000
m5d.2xlarge	Hingga 18.000
m5d.4xlarge	Hingga 30.000
r5.large	Hingga 5.000
r5.xlarge	Hingga 10.000
r5.2xlarge	Hingga 18.000
r5.4xlarge	Hingga 30.000
r5d.large	Hingga 5.000
r5d.xlarge	Hingga 10.000
r5d.2xlarge	Hingga 18.000
r5d.4xlarge	Hingga 30.000

Kuota pada pemeriksaan kondisi

Entitas	Kuota

Entitas	Kuota
Pemeriksaan kondisi	200 pemeriksaan kesehatan aktif per AWS akun Meminta kuota yang lebih tinggi.
Pemeriksaan kondisi anak yang dapat dipantau oleh pemeriksaan kondisi yang dihitung	255
Panjang total maksimum header dalam merespons permintaan pemeriksaan kondisi	16.384 byte (16K)

Kuota pada konfigurasi log kueri

Entitas	Kuota
Konfigurasi log kueri	1 per zona yang di-hosting

Kuota tentang kebijakan alur lalu lintas dan catatan kebijakan

Entitas	Kuota
Kebijakan lalu lintas	50 per AWS akun Meminta kuota yang lebih tinggi.
Untuk informasi selengkapnya tentang alur lalu lintas Route 53, lihat Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS.	
Versi kebijakan lalu lintas	1.000 per kebijakan lalu lintas

Entitas	Kuota
Catatan kebijakan lalu lintas (disebut sebagai “instans kebijakan” di API Route 53,, AWS SDKs AWS Command Line Interface, dan AWS Tools for Windows PowerShell)	5 per AWS akun Meminta kuota yang lebih tinggi.

Kuota pada set delegasi dapat digunakan kembali

Entitas	Kuota
Set delegasi yang dapat digunakan kembali	100 per AWS akun Meminta kuota yang lebih tinggi.

Kuota pada Profil Route 53

Entitas	Kuota
Jumlah Route 53 Profil per Akun AWS Wilayah	5 Meminta kuota yang lebih tinggi.
Jumlah VPCs yang dapat dikaitkan dengan Profil	1000 Meminta kuota yang lebih tinggi.
Jumlah grup aturan DNS Firewall per Profil	5
Jumlah aturan Resolver per Profil	1000 Meminta kuota yang lebih tinggi.

Entitas	Kuota
Jumlah zona yang dihosting pribadi per Profil	5000 Meminta kuota yang lebih tinggi.
Jumlah konfigurasi pencatatan kueri VPC Resolver per Profil	2

Maksimum pada permintaan API

Permintaan API Amazon Route 53 tunduk pada jumlah maksimum berikut.

Topik

- [Jumlah elemen dan karakter dalam permintaan `ChangeResourceRecordSets`](#)
- [Frekuensi permintaan API Amazon Route 53](#)
- [Frekuensi permintaan API Route 53 VPC Resolver](#)

Jumlah elemen dan karakter dalam permintaan `ChangeResourceRecordSets`

Elemen `ResourceRecord`

Permintaan tidak dapat berisi lebih dari 1.000 `ResourceRecord` elemen (termasuk catatan alias). Ketika nilai elemen `Action` adalah `UPSERT`, setiap elemen `ResourceRecord` dihitung dua kali.

Jumlah karakter maksimum

Jumlah karakter (termasuk spasi) di semua elemen `Value` dalam permintaan tidak dapat lebih dari 32.000 karakter. Ketika nilai elemen `Action` adalah `UPSERT`, setiap karakter dalam elemen `Value` dihitung dua kali.

Frekuensi permintaan API Amazon Route 53

Semua permintaan API Amazon Route 53

Untuk [Amazon Route 53 APIs](#) lima permintaan per detik per AWS akun. Jika Anda mengirimkan lebih dari lima permintaan per detik, Amazon Route 53 mengembalikan kesalahan HTTP 400 (Bad request). Header respons juga mencakup elemen Code dengan nilai Throttling dan elemen Message dengan nilai Rate exceeded.

Note

Jika aplikasi melebihi batas ini, sebaiknya Anda menerapkan backoff eksponensial untuk percobaan ulang. Untuk informasi selengkapnya, lihat [Error Retries dan Exponential Backoff](#) di AWSReferensi Umum Amazon Web Services

Permintaan **ChangeResourceRecordSets**

Jika tidak dapat memproses permintaan sebelum permintaan berikutnya tiba, Route 53 akan menolak permintaan berikutnya untuk zona yang di-hosting yang sama dan mengembalikan kesalahan HTTP 400 (Bad request). Header respons juga mencakup elemen Code dengan nilai PriorRequestNotComplete dan elemen Message dengan nilai The request was rejected because Route 53 was still processing a prior request.

Permintaan **CreateHealthCheck**

Anda dapat mengirimkan satu CreateHealthCheck permintaan setiap 2 detik per Akun AWS.

Frekuensi permintaan API Route 53 VPC Resolver

Semua permintaan

Lima permintaan per detik per AWS akun per Wilayah. Jika Anda mengirimkan lebih dari lima permintaan per detik di Wilayah, VPC Resolver mengembalikan kesalahan HTTP 400 (). Bad request Header respons juga mencakup elemen Code dengan nilai Throttling dan elemen Message dengan nilai Rate exceeded.

 Note

Jika aplikasi melebihi batas ini, sebaiknya Anda menerapkan backoff eksponensial untuk percobaan ulang. Untuk informasi selengkapnya, lihat [Error Retries dan Exponential Backoff](#) di AWSReferensi Umum Amazon Web Services

Informasi terkait

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

Topik

- [AWS sumber daya](#)
- [Alat dan pustaka pihak ketiga](#)
- [Antarmuka pengguna grafis](#)

AWS sumber daya

Beberapa panduan bermanfaat, forum, dan sumber daya lainnya tersedia dari Amazon Web Services.

- [Referensi Amazon Route 53](#) – Panduan referensi yang mencakup lokasi skema; deskripsi lengkap tentang tindakan API, parameter, dan jenis data; serta daftar kesalahan yang dihasilkan layanan.
- [AWS::Route53::RecordSet Ketik](#) Panduan AWS CloudFormation Pengguna — Properti untuk menggunakan Amazon Route 53 CloudFormation untuk membuat nama DNS yang disesuaikan untuk CloudFormation tumpukan Anda.
- [Forum Diskusi](#) – Forum berbasis komunitas bagi pengembang untuk membahas pertanyaan teknis terkait Route 53..
- [AWS Support Center](#) — Situs ini menyatukan informasi tentang kasus dukungan terbaru Anda dan hasil dari AWS Trusted Advisor dan pemeriksaan kesehatan, serta menyediakan tautan ke forum diskusi, teknis FAQs, dasbor kesehatan layanan, dan informasi tentang rencana AWS dukungan.
- [AWS Informasi Dukungan Premium](#) — Halaman web utama untuk informasi tentang Dukungan AWS Premium, saluran dukungan respons cepat untuk membantu Anda membangun dan menjalankan aplikasi di Layanan AWS Infrastruktur. one-on-one
- [Hubungi Kami](#) – Tautan untuk pertanyaan tentang tagihan atau akun Anda. Untuk pertanyaan teknis, gunakan forum diskusi atau tautan dukungan di atas.
- [Informasi produk Route 53](#) – Halaman web utama untuk informasi tentang Route 53, termasuk fitur, harga, dan lainnya.
- [Kelas & Lokakarya](#) - Tautan ke kursus berbasis peran dan khusus, selain laboratorium mandiri untuk membantu mempertajam keterampilan Anda AWS dan mendapatkan pengalaman praktis.

- [AWS Pusat Pengembang](#) — Jelajahi tutorial, unduh alat, dan pelajari tentang acara AWS pengembang.
- [AWS Alat Pengembang](#) — Tautan ke alat pengembang SDKs, toolkit IDE, dan alat baris perintah untuk mengembangkan dan mengelola AWS aplikasi.
- [Memulai Pusat Sumber Daya](#) — Pelajari cara menyiapkan Akun AWS, bergabung dengan AWS komunitas, dan meluncurkan aplikasi pertama Anda.
- [Hands-On Tutorial](#) - Ikuti step-by-step tutorial untuk meluncurkan aplikasi pertama Anda. AWS
- [AWS Whitepaper](#) — Tautan ke daftar lengkap AWS whitepaper teknis, yang mencakup topik-topik seperti arsitektur, keamanan, dan ekonomi dan ditulis oleh AWS Solutions Architects atau pakar teknis lainnya.
- [AWS Dukungan Pusat](#) — Hub untuk membuat dan mengelola AWS Dukungan kasus Anda. Juga termasuk tautan ke sumber daya bermanfaat lainnya, seperti forum, teknis FAQs, status kesehatan layanan, dan AWS Trusted Advisor.
- [Dukungan](#)— Halaman web utama untuk informasi tentang Dukungan, saluran dukungan respons cepat untuk membantu Anda membangun dan menjalankan aplikasi di cloud. one-on-one
- [Hubungi Kami](#) – Titik kontak pusat untuk pertanyaan tentang tandaihan AWS , akun, peristiwa, penyalahgunaan, dan masalah lainnya.
- [AWS Ketentuan Situs](#) — Informasi terperinci tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; dan topik lainnya.

Alat dan pustaka pihak ketiga

Selain AWS sumber daya, Anda dapat menemukan berbagai alat dan pustaka pihak ketiga yang berfungsi dengan Amazon Route 53.

- [AmazonRoute53 AppsScript](#) (melalui webos-goodies)

Manajemen spreadsheet Google dari Amazon Route 53.

- [AWS Komponen untuk .NET](#) (via SprightlySoft)

SprightlySoft .NET Component untuk Amazon Web Services dengan dukungan untuk operasi REST dan Route 53.

- [Unduhan API Boto](#) (melalui github)

Antarmuka Boto Python untuk Amazon Web Services.

- [cli53](#) (melalui github)

Antarmuka baris perintah untuk Route 53.

- [API Awan Dasein](#)

API berbasis Java.

- [R53.py](#) (melalui github)

Mempertahankan versi kanonis konfigurasi DNS Anda di bawah kontrol sumber, dan menghitung set minimum perubahan yang diperlukan untuk mengubah konfigurasi.

- [route53d](#)

Front-end DNS untuk API Route 53 (memungkinkan transfer zona inkremental (IXFR)).

- [Route53Manager](#) (melalui github)

Antarmuka berbasis web.

- [Ruby Fog](#) (melalui github)

Pustaka layanan cloud Ruby.

- [WebService: :Amazon: :Route53 \(melalui CPAN\)](#)

Antarmuka Perl untuk API Amazon Route 53.

Antarmuka pengguna grafis

Alat pihak ketiga berikut menyediakan antarmuka pengguna grafis (GUIs) untuk bekerja dengan Amazon Route 53:

- [R53 Rubah](#)
- [Ylastik](#)

Riwayat dokumen

Entri berikut menjelaskan perubahan penting dalam setiap rilis dokumentasi Route 53. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Topik

- [Rilis 2025](#)
- [Rilis 2024](#)
- [Rilis 2023](#)
- [Rilis 2022](#)
- [Rilis 2021](#)
- [Rilis 2020](#)
- [Rilis 2018](#)
- [Rilis 2017](#)
- [Rilis 2016](#)
- [Rilis 2015](#)
- [Rilis 2014](#)
- [Rilis 2013](#)
- [Rilis 2012](#)
- [Rilis 2011](#)
- [Rilis 2010](#)

Rilis 2025

Desember 15, 2025

Menambahkan CloudWatch metrik terperinci untuk titik akhir Resolver Route 53. Metrik baru ini memberikan kemampuan pemantauan yang ditingkatkan di tingkat Antarmuka Jaringan Resolver dan Server Nama Target, termasuk latensi respons P90 dari kueri DNS, pelacakan status respons SERVFAIL, NXDOMAIN, REFUSED, dan FORMERR, dan pemantauan ketersediaan server nama target untuk titik akhir Resolver keluar. Untuk informasi selengkapnya, lihat [CloudWatch Metrik Terperinci untuk Route 53 VPC Resolver](#).

Juni 26, 2025

Ditambahkan `ResolverEndpointCapacityStatus` ke `AWS/Route53Resolver` namespace. Untuk informasi selengkapnya, lihat [Metrik untuk titik akhir Route 53 VPC Resolver](#).

Juni 25, 2025

Amazon Route 53 sekarang mendukung catatan alias untuk titik akhir domain kustom layanan VPC Lattice. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke titik akhir domain layanan Amazon VPC Lattice](#).

Juni 24, 2025

Anda sekarang dapat menggunakan delegasi masuk dan keluar dengan VPC Resolver. Untuk informasi selengkapnya, lihat [Bagaimana DNS resolver di jaringan Anda meneruskan kueri DNS ke titik akhir Resolver](#).

01 Juni 2025

Menambahkan izin `cloudwatch:GetMetricData`, `tag:GetResources`, `es:ListDomainNames`, `es:DescribeDomains`, `cloudfront:GetDistributionTenantByDomain`, `cloudfront:GetConnectionGroup` dan `lightsail:GetContainerServices`. Izin ini memungkinkan Anda mengambil hingga 500 metrik pemeriksaan CloudWatch kesehatan, hingga 100 nama pemeriksaan kesehatan, mendapatkan konfigurasi domain untuk domain Layanan Amazon yang ditentukan, dan mencantumkan nama semua domain OpenSearch Layanan Amazon yang dimiliki oleh pengguna saat ini di Wilayah aktif, ambil distribusi CloudFront multi-penyewa, dan dapatkan OpenSearch layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola: AmazonRoute 53 FullAccess](#).

April 28, 2025

Anda sekarang dapat mengaitkan titik akhir VPC antarmuka ke Route 53 Profiles. Untuk informasi selengkapnya, lihat [Mengaitkan titik akhir VPC antarmuka ke Profil Route 53](#).

April 28, 2025

Anda sekarang dapat menambahkan catatan alias ke penyewa CloudFront distribusi. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#).

Februari 27, 2025

Memperbarui panduan Route 53 dengan pengalaman konsol baru untuk Arus Lalu Lintas. Untuk informasi selengkapnya, lihat [Membuat dan mengelola kebijakan lalu lintas](#) dan [Membuat dan mengelola catatan kebijakan](#).

Januari 14, 2025

Amazon Route 53 sekarang mendukung catatan alias untuk titik akhir domain kustom OpenSearch Layanan. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke titik akhir domain OpenSearch Layanan Amazon](#).

Januari 13, 2025

Menambahkan temuan Resolver DNS Firewall ke Security Hub CSPM. Untuk informasi selengkapnya, lihat [Mengirim temuan dari Resolver DNS Firewall ke Security Hub CSPM](#).

Rilis 2024

November 15, 2024

Ditambahkan Resolver DNS Firewall Advanced, serangkaian fitur baru pada Resolver DNS Firewall yang memungkinkan Anda mengidentifikasi dan memblokir lalu lintas DNS yang terkait dengan ancaman DNS tingkat lanjut, seperti tunneling DNS, Domain Generation Algorithm (DGA), dan Dictionary DGA berbasis ancaman. Untuk informasi selengkapnya, lihat [Resolver DNS Firewall Lanjutan](#).

Oktober 29, 2024

Menambahkan dukungan untuk jenis catatan DNS HTTPS, SSHFP, SVCB, dan TLSA. Untuk informasi selengkapnya, lihat [Tipe data DNS yang didukung](#).

Oktober 3, 2024

Menambahkan dukungan untuk Service Name Indication (SNI) untuk endpoint DoH Outbound Resolver. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit aturan](#).

September 3, 2024

Anda sekarang dapat menggunakan kondisi `route53:VPCs` kebijakan untuk memberikan akses halus untuk mengelola asosiasi zona yang dihosting. VPCs Untuk informasi selengkapnya, lihat [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#).

Agustus 27, 2024

AmazonRoute53ProfilesFullAccess menambahkan izin untuk GetProfilePolicy dan PutProfilePolicy. Ini adalah tindakan IAM khusus izin. Jika kepala sekolah IAM tidak memiliki izin ini diberikan, kesalahan akan terjadi saat mencoba membagikan Profil menggunakan layanan. AWS RAM Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola: AmazonRoute53 ProfilesFullAccess](#).

Agustus 27, 2024

AmazonRoute53ProfilesReadOnlyAccess menambahkan izin untuk GetProfilePolicy. Ini adalah tindakan IAM khusus izin. Jika kepala sekolah IAM tidak memiliki izin ini diberikan, kesalahan akan terjadi ketika mencoba mengakses kebijakan Profil menggunakan layanan. AWS RAM Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola: AmazonRoute 53 ProfilesReadOnlyAccess](#).

Agustus 5, 2024

Menambahkan id pernyataan (Sid) untuk mengidentifikasi kebijakan terkelola secara unik. AmazonRoute53ResolverFullAccess Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola: AmazonRoute 53 ResolverFullAccess](#).

Agustus 5, 2024

Menambahkan id pernyataan (Sid) untuk mengidentifikasi kebijakan terkelola secara unik. AmazonRoute53ResolverReadOnlyAccess Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola: AmazonRoute 53 ResolverReadOnlyAccess](#).

Juli 18, 2024

Memperbarui seluruh panduan Route 53 dengan pengalaman konsol baru untuk pemeriksaan kesehatan. Untuk informasi selengkapnya, lihat [Membuat, memperbarui, dan menghapus pemeriksaan kondisi](#).

April 30, 2024

Anda sekarang dapat memutuskan apakah aturan DNS Firewall akan memeriksa (default), atau mempercayai rantai pengalihan DNS. Untuk informasi selengkapnya, lihat [Resolver DNS Firewall komponen dan pengaturan](#) dan [Pengaturan aturan di DNS Firewall](#).

April 22, 2024

Anda sekarang dapat menggunakan Route 53 Profiles untuk berbagi konfigurasi DNS-spesifik dengan banyak VPCs dan dengan accounts. AWS Untuk informasi selengkapnya, lihat [Apa itu Profil Amazon Route 53?](#).

April 22, 2024

Menambahkan kebijakan terkelola AmazonRoute53ProfilesReadOnlyAccess dan memberikan AmazonRoute53ProfilesFullAccess akses hanya-baca dan penuh ke Profil Amazon Route 53. Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola untuk Amazon Route 53](#).

Februari 5, 2024

Anda sekarang dapat menggunakan Amazon EventBridge untuk peringatan waktu nyata dengan DNS Firewall. Untuk informasi selengkapnya, lihat [Mengelola peristiwa Resolver DNS Firewall menggunakan Amazon EventBridge](#).

Januari 9, 2024

Anda sekarang dapat menggunakan jenis kueri DNS sebagai nilai opsional untuk aturan DNS Firewall untuk membedakan respons aturan untuk jenis kueri DNS tertentu. Untuk informasi selengkapnya, lihat [Resolver DNS Firewall komponen dan pengaturan](#) dan [Pengaturan aturan di DNS Firewall](#).

Januari 9, 2024

Anda sekarang dapat menggunakan Quick create record atau Create record wizard untuk membuat catatan routing geoproximity. Lihat informasi selengkapnya di [Perutean geoproksimitas](#), [Nilai khusus untuk catatan geoproximity](#), dan [Nilai khusus untuk catatan alias geoproximity](#).

Rilis 2023

20 Desember 2023

Anda sekarang dapat menggunakan DNS melalui HTTPS dengan titik akhir Resolver. Untuk informasi selengkapnya, lihat [Memilih protokol untuk titik akhir](#).

Juli 20, 2023

Amazon Route 53 di Outposts sekarang tersedia di AWS Outposts rak. Ini termasuk Resolver VPC yang menyimpan semua kueri DNS yang berasal dari file. AWS Outposts Anda juga dapat

mengatur konektivitas hibrid antara Outpost dan resolver DNS lokal saat menerapkan titik akhir masuk dan keluar. Untuk informasi selengkapnya, lihat [Apa itu Amazon Route 53 di Outposts?](#).

Juli 19, 2023

Anda sekarang dapat menggunakan Local Zones dengan perutean geoproximity (hanya arus lalu lintas) setelah Anda mengaktifkannya. Untuk informasi selengkapnya, lihat [Perutean geoproksimitas](#) dan [Format Dokumen Kebijakan Lalu Lintas](#).

22 Maret 2023

Memperbarui seluruh panduan Route 53 dengan pengalaman konsol baru untuk domain. Anda juga dapat menggunakan pengalaman konsol baru untuk mentransfer domain dari satu Akun AWS ke yang lain Akun AWS. Untuk informasi selengkapnya, lihat [Mendaftarkan domain baru](#) dan [Mentransfer domain](#).

10 Maret 2023

Anda sekarang dapat terhubung ke sumber daya Anda dengan menggunakan IPv4, IPv6, atau dual-stack endpoint dengan Route 53 VPC Resolver. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir masuk](#) dan [Nilai yang Anda tentukan ketika membuat atau mengedit titik akhir keluar](#).

Rilis 2022

21 September 2022

Anda sekarang dapat menggunakan kondisi kebijakan untuk memberi pengguna akses halus untuk memperbarui kumpulan rekaman sumber daya di Amazon Route 53. Untuk informasi selengkapnya, lihat [Menggunakan ketentuan kebijakan IAM untuk kontrol akses terperinci](#).

30 Agustus 2022

Amazon Route 53 sekarang mendukung catatan alias untuk AWS App Runner layanan yang dibuat setelah 1 Agustus 2022. Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke layanan AWS App Runner](#).

1 Juni 2022

Opsi perutean berbasis IP sekarang tersedia di Amazon Route 53. Untuk informasi selengkapnya, lihat [Perutean berbasis IP](#).

16 Maret 2022

Opsi perutean berbasis geolokasi dan latensi sekarang didukung untuk zona host pribadi di Amazon Route 53. Untuk informasi selengkapnya, lihat [Pertimbangan saat bekerja dengan zona yang di-hosting privat](#).

Januari 25, 2022

Proses untuk mengubah kepemilikan untuk .com.au dan .net.au TLDs telah disederhanakan untuk mencakup menanggapi dua email (oleh pendaftar lama dan baru) dan tidak termasuk mengisi formulir. Untuk informasi selengkapnya, lihat [.com.au \(Australia\)](#) dan [.net.au \(Australia\)](#).

Rilis 2021

26 Oktober 2021

Menambahkan dukungan untuk menonaktifkan aturan DNS terbalik default dengan Amazon Route 53. Anda sekarang dapat menonaktifkan pembuatan aturan ini dan sebagai gantinya meneruskan kueri untuk ruang nama DNS terbalik ke server eksternal jika diinginkan. Untuk informasi selengkapnya, lihat [Aturan penerusan untuk kueri DNS terbalik di VPC Resolver](#).

1 September 2021

Menambahkan topik baru untuk memulai yang memandu Anda membuat CloudFront distribusi Amazon untuk situs web statis. Untuk informasi selengkapnya, lihat [Gunakan CloudFront distribusi Amazon untuk melayani situs web statis](#).

14 Juli 2021

Mulai melacak kebijakan AWS terkelola untuk Amazon Route 53. Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola untuk Amazon Route 53](#).

31 Maret 2021

Ditambahkan Resolver DNS Firewall. Dengan DNS Firewall Anda dapat memberikan perlindungan untuk permintaan DNS keluar dari Anda. VPCs Untuk informasi selengkapnya, lihat [Menggunakan DNS Firewall untuk menyaring lalu lintas DNS keluar](#).

Rilis 2020

17 Desember 2020

Menambahkan dukungan untuk penandatanganan DNSSEC untuk Route 53 VPC Resolver. Untuk informasi selengkapnya, lihat [Mengonfigurasi penandatanganan DNSSEC di Amazon Route 53](#).

Ditambahkan dukungan untuk validasi DNSSEC untuk Route 53 VPC Resolver. Untuk informasi selengkapnya, lihat [Mengaktifkan validasi DNSSEC di Amazon Route 53](#).

23 September 2020

Pembaruan seluruh panduan Route 53 dengan pengalaman konsol baru. Untuk informasi selengkapnya, lihat [Apa itu Amazon Route 53?](#).

1 September 2020

Tambahan dukungan untuk log kueri Resolver. Untuk informasi selengkapnya, lihat [Pencatatan kueri penyelesai](#).

Rilis 2018

20 Desember 2018

Anda dapat membuat catatan alias Route 53 yang merutekan lalu lintas ke API Gateway APIs atau ke titik akhir antarmuka Amazon VPC. Untuk informasi selengkapnya, lihat [Nilai/rutekan lalu lintas ke](#).

28 November 2018

Route 53 Auto Naming (juga dikenal sebagai Service Discovery) sekarang menjadi layanan terpisah AWS Cloud Map. Lihat informasi selengkapnya di [Panduan Developer AWS Cloud Map](#).

19 November 2018

Anda dapat menggunakan Route 53 Resolver untuk mengonfigurasi resolusi DNS antara VPC dan jaringan melalui Direct Connect atau koneksi VPN. (Resolver adalah nama baru untuk layanan DNS rekursif yang disediakan untuk semua pelanggan secara default di Amazon Virtual Private Cloud (Amazon VPC).) Hal ini memungkinkan Anda meneruskan kueri DNS dari penyelesai di jaringan Anda ke Route 53 Resolver. Resolver juga memungkinkan Anda

meneruskan kueri untuk nama domain yang dipilih (example.com) dan nama subdomain (api.example.com) dari VPC ke penyelesai di jaringan Anda. Untuk informasi selengkapnya, lihat [Apa itu Route 53 VPC Resolver?](#).

7 November 2018

Saat menggunakan alur lalu lintas Route 53 dan perutean jarak geografis, Anda dapat menggunakan peta interaktif untuk memvisualisasikan cara pengguna akhir dirutekan ke titik akhir Anda di seluruh dunia. Untuk informasi selengkapnya, lihat [Melihat peta yang menunjukkan efek pengaturan geoproximity](#).

18 Oktober 2018

Anda dapat menggunakan konsol dan API Route 53 untuk menonaktifkan pemeriksaan kondisi Route 53 secara sementara. Hal ini memudahkan Anda menjeda pemantauan titik akhir, seperti server web, sehingga Anda dapat melakukan pemeliharaan tanpa memicu alarm atau menghasilkan log atau pesan status yang tidak perlu. Untuk informasi selengkapnya, lihat "Dinonaktifkan" di [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#). Fitur ini tersedia untuk ketiga jenis pemeriksaan kesehatan Route 53: pemeriksaan kesehatan yang memantau titik akhir, pemeriksaan kesehatan yang memantau pemeriksaan kesehatan lainnya, dan pemeriksaan kesehatan yang memantau CloudWatch alarm.

13 Maret 2018

Jika menggunakan penamaan otomatis, kini Anda dapat menggunakan pemeriksa kondisi pihak ketiga untuk mengevaluasi kondisi sumber daya. Hal ini berguna ketika sumber daya tidak tersedia melalui internet, misalnya, karena instans berada dalam Amazon VPC. Untuk informasi selengkapnya, lihat [HealthCheckCustomConfig](#) di Referensi API Amazon Route 53.

9 Maret 2018

IAM kini menyertakan kebijakan terkelola untuk penamaan otomatis. Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola untuk Amazon Route 53](#).

6 Februari 2018

Anda sekarang dapat mengonfigurasi penamaan otomatis untuk membuat catatan alias yang merutekan lalu lintas ke penyeimbang beban ELB atau untuk membuat catatan CNAME. Untuk informasi selengkapnya, lihat [Atribut](#) dalam dokumentasi untuk [RegisterInstance](#) API di Referensi API Amazon Route 53.

Rilis 2017

5 Desember 2017

Kini Anda dapat menggunakan API penamaan otomatis Route 53 untuk menyediakan instans bagi layanan mikro. Penamaan otomatis memungkinkan Anda membuat catatan DNS secara otomatis dan, secara opsional, pemeriksaan kondisi berdasarkan templat yang Anda tetapkan. Untuk informasi selengkapnya, lihat [Apa itu AWS Cloud Map?](#) di Panduan AWS Cloud Map Pengembang.

16 November 2017

Kini Anda bisa mendapatkan kuota saat ini secara terprogram di sumber daya Route 53 seperti zona yang di-hosting dan pemeriksaan kondisi, serta jumlah setiap sumber daya yang saat ini Anda gunakan. Untuk informasi selengkapnya, lihat [GetAccountLimitGetHostedZoneLimit](#), dan [GetReusableDelegationSetLimit](#) di Referensi API Amazon Route 53.

3 Oktober 2017

Route 53 sekarang menjadi layanan yang memenuhi syarat HIPAA. Untuk informasi selengkapnya, lihat [Validasi kepatuhan untuk Amazon Route 53](#).

29 September 2017

Kini Anda dapat memeriksa secara pemrograman apakah domain dapat ditransfer ke Route 53. Untuk informasi selengkapnya, lihat [CheckDomainTransferability](#) di Referensi API Amazon Route 53.

11 September 2017

Anda sekarang dapat membuat catatan alias Route 53 yang merutekan lalu lintas internet ke Elastic Load Balancing Network Load Balancers. Untuk informasi selengkapnya tentang catatan, lihat [Memilih antara catatan alias dan nonalias](#).

7 September 2017

Jika menggunakan Route 53 sebagai layanan DNS otoritatif publik, kini Anda dapat mencatat kueri DNS yang diterima Route 53. Untuk informasi selengkapnya, lihat [Pencatatan kueri DNS publik](#).

1 September 2017

Jika Anda menggunakan arus lalu lintas Route 53, Anda sekarang dapat menggunakan perutean geoproximity, yang memungkinkan Anda merutekan lalu lintas berdasarkan jarak fisik antara

pengguna dan sumber daya Anda. Anda juga dapat merutekan lebih banyak atau lebih sedikit lalu lintas ke setiap sumber daya dengan menentukan bias positif atau negatif. Untuk informasi selengkapnya, lihat [Perutean geoproksimitas](#).

21 Agustus 2017

Kini Anda dapat menggunakan Route 53 untuk membuat catatan Otorisasi Otoritas Sertifikasi (CAA), yang memungkinkan Anda menentukan otoritas sertifikat yang dapat menerbitkan sertifikat untuk domain dan subdomain Anda. Untuk informasi selengkapnya, lihat [Jenis catatan CAA](#).

18 Agustus 2017

Kini Anda dapat mentransfer sejumlah besar domain ke Route 53 menggunakan konsol Route 53. Untuk informasi selengkapnya, lihat [Mentransfer pendaftaran untuk domain ke Amazon Route 53](#).

Parquet

Saat Anda mendaftarkan domain, pendaftar untuk beberapa domain tingkat atas (TLDs) mengharuskan Anda memverifikasi bahwa Anda menetapkan alamat email yang valid untuk kontak pendaftar. Kini Anda dapat mengirim email verifikasi dan mendapatkan konfirmasi bahwa Anda berhasil memverifikasi alamat email selama proses pendaftaran domain. Untuk informasi selengkapnya, lihat [Mendaftarkan domain baru](#).

21 Juni 2017

Jika ingin merutekan lalu lintas hampir secara acak ke beberapa sumber daya, seperti server web, kini Anda dapat membuat satu catatan jawaban multinilai untuk setiap sumber daya dan, secara opsional, mengaitkan pemeriksaan kondisi Route 53 dengan setiap catatan. Route 53 merespons kueri DNS dengan maksimal delapan catatan sehat untuk merespons setiap kueri DNS, dan memberikan jawaban yang berbeda ke penyelesaian DNS yang berbeda. Untuk informasi selengkapnya, lihat [Perutean jawaban multinilai](#).

10 April 2017

Jika menggunakan konsol Route 53 untuk mentransfer pendaftaran domain ke Route 53, kini Anda dapat memilih salah satu opsi berikut untuk mengaitkan server nama bagi layanan DNS untuk domain dengan pendaftaran domain yang ditransfer:

- Menggunakan server nama untuk zona yang di-hosting Route 53 yang Anda pilih
- Menggunakan server nama bagi layanan DNS saat ini untuk domain
- Menggunakan server nama yang Anda tentukan

Route 53 secara otomatis mengaitkan server nama ini dengan pendaftaran domain yang ditransfer.

Rilis 2016

21 November 2016

Anda sekarang dapat membuat pemeriksaan kesehatan yang menggunakan IPv6 alamat untuk memeriksa kesehatan titik akhir. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

15 November 2016

Kini Anda dapat menggunakan tindakan API Route 53 untuk mengaitkan Amazon VPC yang Anda buat menggunakan satu akun dengan zona yang di-hosting privat yang Anda buat menggunakan akun lain. Untuk informasi selengkapnya, lihat [Mengaitkan VPC Amazon dan zona host pribadi yang Anda buat dengan akun berbeda AWS](#).

30 Agustus 2016

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- Catatan Name Authority Pointer (NAPTR) – Kini Anda dapat membuat catatan NAPTR, yang digunakan oleh aplikasi Dynamic Delegation Discovery System (DDDS) untuk mengubah satu nilai ke nilai lain atau untuk mengganti satu nilai dengan nilai lain. Misalnya, salah satu penggunaan umum adalah mengubah nomor telepon menjadi SIP URIs. Untuk informasi selengkapnya, lihat [Jenis catatan NAPTR](#).
- Alat uji kueri DNS – Kini Anda dapat mensimulasikan kueri DNS untuk catatan dan melihat nilai yang dikembalikan Route 53. Untuk catatan geolokasi dan latensi, Anda juga dapat mensimulasikan permintaan dari alamat IP and/or klien penyelesai DNS tertentu untuk mengetahui respons apa yang akan dikembalikan Route 53 ke klien dengan alamat IP resolver tersebut. and/or Untuk informasi selengkapnya, lihat [Memeriksa respons DNS dari Route 53](#).

11 Agustus, 2016

Dengan rilis ini, Anda dapat membuat catatan alias yang merutekan lalu lintas ke Application Load Balancer ELB. Prosesnya sama dengan Classic Load Balancer. Untuk informasi selengkapnya, lihat [Nilai/rutekan lalu lintas ke](#).

9 Agustus 2016

Dengan rilis ini, Route 53 menambahkan dukungan untuk DNSSEC bagi pendaftaran domain. DNSSEC memungkinkan Anda melindungi domain Anda dari serangan spoofing DNS, yang juga dikenal sebagai serangan. man-in-the-middle Untuk informasi selengkapnya, lihat [Mengonfigurasi DNSSEC untuk domain](#).

7 Juli 2016

Kini Anda dapat memperpanjang pendaftaran domain secara manual dan mendaftarkan domain dengan periode pendaftaran awal yang lebih lama dibandingkan periode pendaftaran minimum yang ditentukan oleh registri. Untuk informasi selengkapnya, lihat [Memperpanjang masa pendaftaran untuk domain](#).

6 Juli 2016

Jika Anda adalah pelanggan AISPL dengan alamat kontak di India, kini Anda dapat menggunakan Route 53 untuk mendaftarkan domain. Untuk informasi lebih lanjut, lihat [Mengelola Akun di India](#).

26 Mei 2016

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- Laporan penagihan domain – Kini Anda dapat mengunduh laporan yang mencantumkan semua biaya pendaftaran domain, menurut domain, untuk jangka waktu tertentu. Laporan ini mencakup semua operasi pendaftaran domain yang dikenakan biaya, termasuk mendaftarkan domain, mentransfer domain ke Route 53, memperbarui pendaftaran domain, dan (untuk beberapa TLDs), mengubah pemilik domain. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:
 - Konsol Route 53 – Lihat [Mengunduh laporan penagihan domain](#)
 - Route 53 API — Lihat [ViewBilling](#) di Referensi API Amazon Route 53.
- Baru TLDs — Anda sekarang dapat mendaftarkan domain yang memiliki yang berikut TLDs: .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website, dan .uk. Untuk informasi selengkapnya, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).
- Baru APIs untuk pendaftaran domain — Untuk operasi yang memerlukan konfirmasi bahwa alamat email untuk kontak pendaftar valid, seperti mendaftarkan domain baru, Anda sekarang dapat secara terprogram menentukan apakah kontak pendaftar telah mengklik tautan di email konfirmasi dan, jika tidak, apakah tautan tersebut masih valid. Anda juga dapat meminta secara terprogram agar kami mengirim email konfirmasi lain. Untuk informasi selengkapnya, lihat dokumentasi berikut di referensi API Amazon Route 53:
 - [GetContactReachabilityStatus](#)
 - [ResendContactReachabilityEmail](#)

5 April 2016

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- Pemeriksaan kesehatan berdasarkan CloudWatch metrik — Anda sekarang dapat membuat pemeriksaan kesehatan yang didasarkan pada status alarm dari CloudWatch metrik apa pun. Hal ini berguna untuk memeriksa kondisi titik akhir yang tidak dapat dijangkau dengan pemeriksaan kondisi Route 53 standar, seperti instans dalam Amazon Virtual Private Cloud (VPC) yang hanya memiliki alamat IP privat. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:
 - Konsol Route 53 – Lihat [Memantau CloudWatch alarm](#) dalam topik "Nilai yang Anda Tentukan Saat Membuat atau Memperbarui Pemeriksaan Kondisi".
 - Route 53 API — Lihat [CreateHealthCheck](#) dan [UpdateHealthCheck](#) di Referensi API Amazon Route 53.
- Lokasi pemeriksaan kondisi yang dapat dikonfigurasi – Kini Anda dapat memilih wilayah pemeriksaan kondisi Route 53 yang memeriksa kondisi sumber daya Anda, yang mengurangi beban pada titik akhir dari pemeriksaan kondisi. Hal ini berguna jika pelanggan Anda terkonsentrasi di satu atau beberapa wilayah geografis. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:
 - Konsol Route 53 – Lihat [Konfigurasi lanjutan \("Pantau Titik Akhir" saja\)](#) dalam topik "Nilai yang Anda Tentukan Saat Membuat atau Memperbarui Pemeriksaan Kondisi".
 - Route 53 API - Lihat Regions elemen untuk [CreateHealthCheck](#) dan [UpdateHealthCheck](#) di Referensi API Amazon Route 53.
- Failover di zona yang di-hosting secara privat – Kini Anda dapat membuat failover dan catatan alias failover di zona yang di-hosting secara privat. Ketika menggabungkan fitur ini dengan pemeriksaan kondisi berbasis metrik, Anda dapat mengonfigurasi failover DNS bahkan untuk titik akhir yang hanya memiliki alamat IP privat dan tidak dapat dijangkau menggunakan pemeriksaan kondisi standar Route 53. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:
 - Konsol Route 53 – Lihat [Mengonfigurasi failover di zona yang di-hosting secara privat](#).
 - Route 53 API — Lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.
- Catatan alias di zona yang di-hosting secara privat – Di masa lalu, Anda dapat membuat catatan alias yang merutekan kueri DNS hanya ke catatan Route 53 lainnya dalam zona yang di-hosting yang sama. Dengan rilis ini, Anda juga dapat membuat catatan alias yang merutekan kueri DNS ke lingkungan Elastic Beanstalk yang memiliki subdomain regional, penyeimbang beban Elastic Load Balancing, dan bucket Amazon S3. (Anda masih tidak dapat membuat catatan alias yang merutekan kueri DNS ke distribusi.) CloudFront Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Konsol Route 53 – Lihat [Memilih antara catatan alias dan nonalias](#).
- Route 53 API — Lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.

23 Februari 2016

Jika membuat atau memperbarui pemeriksaan kondisi HTTPS, kini Anda dapat mengonfigurasi Route 53 untuk mengirimkan nama host ke titik akhir selama negosiasi TLS. Hal ini memungkinkan endpoint untuk menanggapi permintaan HTTPS dengan SSL/TLS sertifikat yang berlaku. Untuk informasi selengkapnya, lihat deskripsi SNI di [Konfigurasi lanjutan \("Pantau Titik Akhir" saja\)](#) bidang di topik “Nilai yang Anda Tentukan Saat Membuat atau Memperbarui Pemeriksaan Kesehatan”. Untuk informasi tentang cara mengaktifkan SNI saat Anda menggunakan API untuk membuat atau memperbarui pemeriksaan kesehatan, lihat [CreateHealthCheck](#) dan [UpdateHealthCheck](#) di Referensi API Amazon Route 53.

27 Januari 2016

Anda sekarang dapat mendaftarkan domain untuk lebih dari 100 domain tingkat atas tambahan (TLDs) seperti .accountants, .band, dan .city. Untuk daftar lengkap dukungan TLDs, lihat [Domain yang dapat Anda daftarkan dengan Amazon Route 53](#).

19 Januari 2016

Kini Anda dapat membuat catatan alias yang merutekan lalu lintas ke lingkungan Elastic Beanstalk. Untuk informasi tentang membuat catatan menggunakan konsol Route 53, lihat [Membuat catatan dengan menggunakan konsol Amazon Route 53](#). Untuk informasi tentang menggunakan API untuk membuat rekaman, lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.

Rilis 2015

3 Desember 2015

Konsol Route 53 kini menyertakan editor visual yang memungkinkan Anda membuat konfigurasi perutean yang kompleks dengan cepat menggunakan kombinasi kebijakan perutean tertimbang, latensi, failover, dan geolokasi Route 53. Anda kemudian dapat mengaitkan konfigurasi dengan satu atau lebih nama domain (seperti example.com) atau nama subdomain (seperti www.example.com), di zona yang di-hosting yang sama atau di beberapa zona yang di-hosting. Selain itu, Anda dapat memulihkan pembaruan jika konfigurasi baru tidak memiliki performa seperti yang Anda harapkan. Fungsionalitas yang sama tersedia dengan menggunakan Route 53 API AWS SDKs, AWS CLI, dan AWS Tools for Windows PowerShell. Untuk informasi tentang

menggunakan editor visual, lihat [Menggunakan Arus Lalu Lintas untuk merutekan lalu lintas DNS](#). Untuk informasi tentang menggunakan API untuk membuat konfigurasi alur lalu lintas, lihat [Referensi API Amazon Route 53](#).

19 Oktober 2015

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- Pendaftaran domain untuk domain.com dan .net oleh Amazon Registrar, Inc. — Amazon sekarang menjadi registrar terakreditasi ICANN untuk domain tingkat atas.com dan .net () TLDs melalui Amazon Registrar, Inc. Ketika Anda menggunakan Route 53 untuk mendaftarkan domain.com atau .net, Amazon Registrar akan menjadi pencatat catatan dan akan terdaftar sebagai “Pendaftar Sponsor” dalam hasil kueri Whois Anda. Untuk informasi tentang cara menggunakan Route 53 guna mendaftarkan domain, lihat [Mendaftarkan dan mengelola domain menggunakan Amazon Route 53](#).
- Perlindungan privasi untuk domain .com dan .net – Saat Anda mendaftarkan domain .com atau .net dengan Route 53, semua informasi pribadi Anda, termasuk nama depan dan belakang, kini disembunyikan. Nama depan dan belakang tidak disembunyikan untuk domain lain yang Anda daftarkan dengan Route 53. Untuk informasi selengkapnya tentang perlindungan privasi, lihat [Mengaktifkan atau menonaktifkan perlindungan privasi untuk informasi kontak untuk domain](#).

15 September 2015

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- Pemeriksaan kondisi yang dihitung – Kini Anda dapat membuat pemeriksaan kondisi yang statusnya ditentukan oleh status kondisi pemeriksaan kondisi lainnya. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#). Selain itu, lihat [CreateHealthCheck](#) di Referensi API Amazon Route 53.
- Pengukuran latensi untuk pemeriksaan kondisi – Kini Anda dapat mengonfigurasi Route 53 untuk mengukur latensi antara pemeriksa kondisi dan titik akhir Anda. Data latensi muncul di CloudWatch grafik Amazon di konsol Route 53. Untuk mengaktifkan pengukuran latensi bagi pemeriksaan kondisi baru, lihat pengaturan Pengukuran latensi di bawah [Konfigurasi lanjutan \("Pantau Titik Akhir" saja\)](#) dalam topik [Nilai yang Anda tentukan saat membuat atau memperbarui pemeriksaan kondisi](#). (Anda tidak dapat mengaktifkan pengukuran latensi untuk pemeriksaan kondisi yang ada.) Selain itu, lihat topik MeasureLatency [CreateHealthCheck](#) di Referensi API Amazon Route 53.
- Pembaruan dasbor pemeriksaan kesehatan di konsol Route 53 — Dasbor untuk memantau pemeriksaan kesehatan telah ditingkatkan dalam berbagai cara, termasuk CloudWatch grafik

untuk memantau latensi antara pemeriksaan kesehatan Route 53 dan titik akhir Anda. Untuk informasi selengkapnya, lihat [Memantau status pemeriksaan kondisi dan mendapatkan notifikasi](#).

3 Maret 2015

Panduan Developer Amazon Route 53 kini menjelaskan cara mengonfigurasi server nama label putih untuk zona yang di-hosting Route 53. Untuk informasi selengkapnya, lihat [Mengonfigurasi server nama label putih](#).

26 Februari 2015

Sekarang Anda dapat menggunakan API Route 53 untuk mencantumkan zona yang dihosting yang terkait dengan AWS akun dalam urutan abjad berdasarkan nama. Anda juga bisa mendapatkan jumlah zona yang di-hosting yang terkait dengan akun. Untuk informasi selengkapnya, lihat [ListHostedZonesByName](#) dan [GetHostedZoneCount](#) di Referensi API Amazon Route 53.

11 Februari 2015

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- **Status Pemeriksaan Kondisi** – Halaman pemeriksaan kondisi di konsol Route 53 kini menyertakan kolom Status yang memungkinkan Anda melihat status keseluruhan semua pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Melihat status pemeriksaan kondisi dan alasan kegagalan pemeriksaan kondisi](#).
- **Integrasi dengan AWS CloudTrail** — Route 53 sekarang berfungsi CloudTrail untuk menangkap informasi tentang setiap permintaan yang dikirimkan AWS akun Anda ke API Route 53. Mengintegrasikan Route 53 dan CloudTrail memungkinkan Anda menentukan permintaan mana yang dibuat ke API Route 53, alamat IP sumber dari mana setiap permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan banyak lagi. Untuk informasi selengkapnya, lihat [Mencatat panggilan API Amazon Route 53 dengan AWS CloudTrail](#).
- **Alarm Cepat untuk Pemeriksaan Kesehatan** — Saat Anda membuat pemeriksaan kesehatan dengan menggunakan konsol Route 53, Anda sekarang dapat secara bersamaan membuat CloudWatch alarm Amazon untuk pemeriksaan kesehatan dan menentukan siapa yang akan diberi tahu ketika Route 53 menganggap titik akhir tidak sehat selama satu menit. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).
- **Penandaan untuk Zona dan Domain yang Di-hosting** – Kini Anda dapat menetapkan tanda, yang umumnya digunakan untuk alokasi biaya, ke zona dan domain yang di-hosting Route 53. Untuk informasi selengkapnya, lihat [Memberi tanda pada sumber daya Amazon Route 53](#).

5 Februari 2015

Kini Anda dapat menggunakan konsol Route 53 guna memperbarui informasi kontak untuk domain. Untuk informasi selengkapnya, lihat [Nilai yang Anda tentukan saat mendaftar atau mentransfer domain](#).

22 Januari 2015

Kini Anda dapat menentukan nama domain yang diinternasionalisasi ketika mendaftarkan nama domain baru dengan Route 53. (Route 53 sudah didukung nama domain yang diinternasionalisasi untuk zona dan catatan yang di-hosting.) Untuk informasi selengkapnya, lihat [Format nama domain DNS](#).

Rilis 2014

25 November 2014

Dengan rilis ini, kini Anda dapat mengedit komentar yang ditentukan untuk zona yang di-hosting ketika Anda membuatnya. Di konsol, Anda cukup klik ikon pensil di samping bidang Komentar dan masukkan nilai baru. Untuk informasi selengkapnya tentang mengubah komentar menggunakan API Route 53, lihat [UpdateHostedZoneComment](#) di Referensi API Amazon Route 53.

5 November 2014

Dengan rilis ini, Route 53 menambahkan fitur baru berikut:

- DNS pribadi untuk VPCs dibuat menggunakan layanan Amazon Virtual Private Cloud — Anda sekarang dapat menggunakan Route 53 untuk mengelola nama domain internal Anda VPCs tanpa mengekspos data DNS ke internet publik. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting privat](#).
- Alasan kegagalan pemeriksaan kondisi – Kini Anda dapat melihat status pemeriksaan kondisi terpilih saat ini, serta detail mengapa pemeriksaan kondisi terakhir gagal, seperti yang dilaporkan oleh setiap pemeriksa kondisi Route 53. Status mencakup kode status HTTP, dan alasan kegagalan mencakup informasi tentang berbagai jenis kegagalan, seperti kegagalan pencocokan string dan waktu respons habis. Untuk informasi selengkapnya, lihat [Melihat status pemeriksaan kondisi dan alasan kegagalan pemeriksaan kondisi](#).
- Set delegasi yang dapat digunakan kembali – Kini Anda dapat menerapkan set dari empat server nama otoritatif yang sama, yang dikenal secara kolektif sebagai set delegasi, ke beberapa zona yang di-hosting yang sesuai dengan nama domain yang berbeda. Ini sangat menyederhanakan proses migrasi layanan DNS ke Route 53 dan mengelola sejumlah

besar zona yang di-hosting. Menggunakan set delegasi dapat digunakan kembali saat ini mengharuskan Anda menggunakan API Route 53 atau SDK AWS . Untuk informasi lebih lanjut, lihat [Referensi API Amazon Route 53](#).

- Peningkatan perutean geolokasi - Kami lebih meningkatkan akurasi perutean geolokasi dengan menambahkan dukungan untuk perpanjangan EDNS0. edns-client-subnet Untuk informasi selengkapnya, lihat [Perutean geolokasi](#).
- Dukungan untuk Signature v4 – Kini Anda dapat menandatangani semua permintaan API Route 53 menggunakan Signature versi 4. Untuk informasi lebih lanjut, lihat [Menandatangani permintaan API Route 53](#) dalam Referensi API Amazon Route 53.

31 Juli 2014

Dengan rilis ini, kini Anda dapat melakukan hal berikut:

- Mendaftarkan domain menggunakan Route 53. Untuk informasi selengkapnya, lihat [Mendaftarkan dan mengelola domain menggunakan Amazon Route 53](#).
- Mengonfigurasi Route 53 untuk merespons kueri DNS berdasarkan lokasi geografis tempat kueri berasal. Untuk informasi selengkapnya, lihat [Perutean geolokasi](#).

2 Juli 2014

Dengan rilis ini, kini Anda dapat melakukan hal berikut:

- Mengedit sebagian besar nilai dalam pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Membuat, memperbarui, dan menghapus pemeriksaan kondisi](#).
- Menggunakan API Route 53 untuk mendapatkan daftar rentang IP yang digunakan pemeriksa kondisi Route 53 untuk memeriksa kondisi sumber daya Anda. Anda dapat menggunakan alamat IP ini untuk mengonfigurasi aturan router dan firewall guna mengizinkan pemeriksa kondisi memeriksa kondisi sumber daya Anda. Untuk informasi selengkapnya, lihat [GetCheckerIpRanges](#) di Referensi API Amazon Route 53.
- Menetapkan tanda alokasi biaya untuk pemeriksaan kondisi, yang juga memungkinkan Anda menetapkan nama untuk pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Penamaan dan penandaan pemeriksaan kondisi](#).
- Gunakan API Route 53 untuk mendapatkan jumlah pemeriksaan kesehatan yang terkait dengan AWS akun Anda. Untuk informasi selengkapnya, lihat [GetHealthCheckCount](#) di Referensi API Amazon Route 53.

30 April 2014

Dengan rilis ini, kini Anda dapat membuat pemeriksaan kondisi dan menggunakan nama domain, alih-alih alamat IP, untuk menentukan titik akhir. Ini berguna ketika alamat IP titik akhir tidak

diperbaiki atau dilayani oleh beberapa IPs, seperti instans Amazon EC2 atau Amazon RDS. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pemeriksaan kondisi](#).

Selain itu, beberapa informasi tentang menggunakan API Route 53 yang sebelumnya muncul dalam Panduan Developer Amazon Route 53 telah dipindahkan. Kini semua dokumentasi API muncul di Referensi API Amazon Route 53.

18 April 2014

Dengan rilis ini, Route 53 meneruskan nilai yang berbeda dalam header Host ketika nilai Port pemeriksaan kondisi adalah 443 dan nilai Protokol adalah HTTPS. Selama pemeriksaan kondisi, Route 53 kini meneruskan header Host ke titik akhir yang berisi nilai bidang Nama Host. Jika Anda membuat pemeriksaan kondisi menggunakan tindakan API `CreateHealthCheck`, ini adalah nilai elemen `FullyQualifiedDomainName`.

Untuk informasi selengkapnya, lihat [Membuat, memperbarui, dan menghapus pemeriksaan kondisi](#).

9 April 2014

Dengan rilis ini, kini Anda dapat melihat persentase pemeriksaan kondisi Route 53 yang saat ini melaporkan bahwa titik akhir sehat.

Selain itu, perilaku metrik Status Pemeriksaan Kesehatan di Amazon CloudWatch sekarang hanya menunjukkan nol (jika titik akhir Anda tidak sehat selama periode waktu tertentu) atau satu (jika titik akhir sehat untuk periode waktu tersebut). Metrik tidak lagi menampilkan nilai antara 0 hingga 1 yang mencerminkan bagian dari pemeriksaan kondisi Route 53 yang melaporkan titik akhir sebagai sehat.

Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

18 Februari 2014

Dengan rilis ini, Route 53 menambahkan fitur berikut:

- Ambang batas failover pemeriksaan kondisi: Kini Anda dapat menentukan berapa banyak kegagalan berturut-turut pada pemeriksaan kondisi titik akhir sebelum Route 53 menganggap titik akhir tidak sehat, antara 1 hingga 10 pemeriksaan berturut-turut. Titik akhir yang tidak sehat harus meneruskan jumlah pemeriksaan yang sama cek agar dianggap sehat. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

- Interval permintaan pemeriksaan kondisi: Kini Anda dapat menentukan seberapa sering Route 53 mengirimkan permintaan ke titik akhir untuk menentukan apakah titik akhir sehat. Pengaturan yang valid adalah 10 detik hingga 30 detik. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

30 Januari 2014

Dengan rilis ini, Route 53 menambahkan fitur berikut:

- Pemeriksaan kondisi pencocokan string HTTP dan HTTPS: Route 53 kini mendukung pemeriksaan kondisi yang menentukan kondisi titik akhir berdasarkan tampilan string yang ditentukan dalam isi respons. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).
- Pemeriksaan kondisi HTTPS: Route 53 kini mendukung pemeriksaan kondisi untuk situs web khusus SSL yang aman. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).
- **UPSERT** untuk tindakan API **ChangeResourceRecordSets**: Jika membuat atau mengubah catatan menggunakan tindakan API ChangeResourceRecordSets, kini Anda dapat menggunakan tindakan UPSERT untuk membuat catatan baru jika tidak terdapat catatan dengan nama dan jenis tertentu, atau untuk memperbarui catatan yang ada. Untuk informasi selengkapnya, lihat [ChangeResourceRecordSets](#) di Referensi API Amazon Route 53.

7 Januari 2014

Dengan rilis ini, Route 53 menambahkan dukungan untuk pemeriksaan kondisi yang menentukan kondisi titik akhir berdasarkan apakah string tertentu muncul dalam isi respons. Untuk informasi selengkapnya, lihat [Bagaimana Amazon Route 53 menentukan apakah pemeriksaan kondisi sehat](#).

Rilis 2013

14 Agustus 2013

Dengan rilis ini, Route 53 menambahkan dukungan untuk membuat catatan dengan mengimpor file zona berformat BIND. Untuk informasi selengkapnya, lihat [Membuat catatan dengan mengimpor file zona](#).

Selain itu, CloudWatch metrik untuk pemeriksaan kesehatan Route 53 telah diintegrasikan ke dalam konsol Route 53 dan disederhanakan. Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

26 Juni 2013

Dengan rilis ini, Route 53 menambahkan dukungan untuk mengintegrasikan pemeriksaan kesehatan dengan CloudWatch metrik sehingga Anda dapat melakukan hal berikut:

- Memverifikasi apakah pemeriksaan kondisi dikonfigurasi dengan benar.
- Meninjau kondisi titik akhir pemeriksaan kondisi selama jangka waktu tertentu.
- Konfigurasi CloudWatch untuk mengirim peringatan Amazon Simple Notification Service (Amazon SNS) saat semua pemeriksaan kesehatan Route 53 menganggap titik akhir yang Anda tentukan tidak sehat.

Untuk informasi selengkapnya, lihat [Memantau pemeriksaan kesehatan menggunakan CloudWatch](#).

11 Juni 2013

Dengan rilis ini, Route 53 menambahkan dukungan untuk membuat catatan alias yang merutekan kueri DNS ke nama domain alternatif untuk distribusi Amazon CloudFront. Anda dapat menggunakan fitur ini untuk nama domain alternatif di zone apex (example.com) dan nama domain alternatif untuk subdomain (www.example.com). Untuk informasi selengkapnya, lihat [Merutekan lalu lintas ke CloudFront distribusi Amazon dengan menggunakan nama domain Anda](#).

30 Mei 2013

Dengan rilis ini, Route 53 menambahkan dukungan untuk mengevaluasi kesehatan penyeimbang beban ELB dan instans Amazon terkait EC2. Untuk informasi selengkapnya, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

28 Maret 2013

Dokumentasi tentang pemeriksaan kondisi dan failover ditulis ulang untuk meningkatkan kegunaan. Untuk informasi selengkapnya, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

11 Februari 2013

Dengan rilis ini, Route 53 menambahkan dukungan untuk failover dan pemeriksaan kondisi. Untuk informasi selengkapnya, lihat [Membuat pemeriksaan kesehatan Amazon Route 53](#).

Rilis 2012

21 Maret 2012

Dengan rilis ini, Route 53 memungkinkan Anda membuat catatan latensi. Untuk informasi selengkapnya, lihat [Perutean berbasis latensi](#).

Rilis 2011

21 Desember 2011

Dengan rilis ini, konsol Route 53 di dalamnya Konsol Manajemen AWS memungkinkan Anda membuat catatan alias dengan memilih Elastic Load Balancer dari daftar alih-alih memasukkan ID zona yang dihosting secara manual dan nama DNS penyeimbang beban. Fungsionalitas baru didokumentasikan dalam Panduan Developer Amazon Route 53.

16 November 2011

Dengan rilis ini, Anda dapat menggunakan konsol Route 53 di Konsol Manajemen AWS untuk membuat dan menghapus zona yang dihosting, dan untuk membuat, mengubah, dan menghapus catatan. Fungsionalitas baru didokumentasikan di seluruh Panduan Developer Amazon Route 53, sebagaimana berlaku.

18 Oktober 2011

Panduan Memulai Amazon Route 53 digabungkan ke dalam Panduan Developer Amazon Route 53, dan Panduan Developer Guide disusun ulang untuk meningkatkan kegunaan.

24 Mei 2011

Rilis Amazon Route 53 ini memperkenalkan catatan alias, yang memungkinkan Anda untuk membuat alias zone apex; catatan tertimbang; API baru (2011-05-05); dan perjanjian tingkat layanan. Selain itu, setelah enam bulan dalam versi beta, Route 53 kini tersedia untuk umum. Untuk informasi lebih lanjut, lihat [Halaman produk Amazon Route 53](#) dan [Memilih antara catatan alias dan nonalias](#) dalam Panduan Developer Amazon Route 53.

Rilis 2010

5 Desember 2010

Ini merupakan rilis pertama dari Panduan Developer Amazon Route 53.

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