
Amazon Route 53

Developer Guide

API Version 2013-04-01



Amazon Route 53: Developer Guide

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon Route 53?	1
How domain registration works	1
How internet traffic is routed to your website or web application	2
Overview of how you configure Amazon Route 53 to route internet traffic for your domain	3
How Amazon Route 53 routes traffic for your domain	3
How Amazon Route 53 checks the health of your resources	5
Amazon Route 53 concepts	6
Domain registration concepts	6
Domain Name System (DNS) concepts	7
Health checking concepts	10
How to get started with Amazon Route 53	11
Related services	11
Accessing Amazon Route 53	11
AWS Identity and Access Management	12
Amazon Route 53 pricing and billing	12
Setting up	13
Sign up for AWS	13
Access your account	13
Access the console	13
Access the API, AWS CLI, AWS Tools for Windows PowerShell, or the AWS SDKs	14
Create an IAM user	14
Set up the AWS Command Line Interface or AWS Tools for Windows PowerShell	15
Download an AWS SDK	16
Getting started	17
Use your domain for a static website	17
Prerequisites	18
Step 1: Register a domain	18
Step 2: Create an S3 bucket for your root domain	20
Step 3 (<i>optional</i>): Create another S3 Bucket, for your subdomain	20
Step 4: Set up your root domain bucket for website hosting	20
Step 5 : (<i>optional</i>): Set up your subdomain bucket for website redirect	21
Step 6: Upload index to create website content	22
Step 7: Edit S3 Block Public Access settings	22
Step 8: Attach a bucket policy	23
Step 9: Test your domain endpoint	23
Step 10: Route DNS traffic for your domain to your website bucket	24
Step 11: Test your website	25
Step 12 (<i>optional</i>): Use Amazon CloudFront to speed up distribution of your content	25
Use an Amazon CloudFront distribution to serve a static website	26
Prerequisites	26
Step 1: Register a domain	26
Step 2: Request a public certificate	28
Step 3: Create an S3 bucket to host your subdomain	29
Step 4 : Create another S3 bucket, for your root domain	29
Step 5: Upload website files to your subdomain bucket	30
Step 6: Set up your root domain bucket for website redirect	30
Step 7: Create an Amazon CloudFront distribution for your subdomain	31
Step 8: Create an Amazon CloudFront distribution for your root domain	31
Step 9: Route DNS traffic for your domain to your CloudFront distribution	32
Step 10 : Test your website	33
Integration with other services	35
Logging, monitoring, and tagging	35
Routing traffic to other AWS resources	35
DNS domain name format	38

Formatting domain names for domain name registration	38
Formatting domain names for hosted zones and records	38
Using an asterisk (*) in the names of hosted zones and records	39
Formatting internationalized domain names	40
Registering domain names	41
Registering domains	41
Registering a new domain	42
Values that you specify when you register or transfer a domain	47
Values that Amazon Route 53 returns when you register a domain	51
Viewing the status of a domain registration	52
Updating settings for a domain	52
Updating contact information and ownership for a domain	52
Enabling or disabling privacy protection for contact information for a domain	57
Enabling or disabling automatic renewal for a domain	59
Locking a domain to prevent unauthorized transfer to another registrar	59
Extending the registration period for a domain	59
Adding or changing name servers and glue records for a domain	61
Renewing registration for a domain	63
Restoring an expired or deleted domain	65
Replacing the hosted zone for a domain	66
Transferring domains	67
Transferring domain registration to Route 53	67
Viewing the status of a domain transfer	78
How transferring a domain to Route 53 affects the expiration date	80
Transferring a domain to a different AWS account	81
Transferring a domain from Route 53	83
Resending authorization and confirmation emails	86
Updating your email address	87
Resending emails	87
Configuring DNSSEC for a domain	89
Overview of how DNSSEC protects your domain	90
Prerequisites and maximums for configuring DNSSEC for a domain	91
Adding public keys for a domain	91
Deleting public keys for a domain	92
Viewing information about domains	93
Deleting a domain name registration	93
Contacting AWS Support about domain registration issues	95
Contacting AWS Support when you can sign in to your AWS account	95
Contacting AWS Support when you can't sign in to your AWS account	96
Downloading a domain billing report	96
Domains that you can register with Amazon Route 53	97
Index to supported top-level domains	98
Generic top-level domains	101
Geographic top-level domains	280
Configuring Amazon Route 53 as your DNS service	325
Making Route 53 the DNS service for an existing domain	325
Making Route 53 the DNS service for a domain that's in use	326
Making Route 53 the DNS service for an inactive domain	331
Configuring DNS routing for a new domain	334
Routing traffic to your resources	335
Routing traffic for subdomains	335
Working with hosted zones	339
Working with public hosted zones	339
Working with private hosted zones	356
Migrating a hosted zone to a different AWS account	363
Working with records	370
Choosing a routing policy	371

Choosing between alias and non-alias records	379
Supported DNS record types	382
Creating records by using the Amazon Route 53 console	392
Values you specify	393
Creating records by importing a zone file	438
Editing records	440
Deleting records	440
Listing records	441
Using traffic flow to route DNS traffic	442
Creating and managing traffic policies	443
Creating and managing policy records	453
Configuring DNSSEC signing	455
Enabling DNSSEC signing and establishing a chain of trust	456
Disabling DNSSEC signing	462
Working with customer managed keys	465
Working with key-signing keys (KSKs)	466
KMS key and ZSK management in Route 53	468
DNSSEC proofs of nonexistence in Route 53	468
Troubleshooting DNSSEC signing	469
Using AWS Cloud Map to create records and health checks	470
DNS constraints and behaviors	470
Maximum response size	470
Authoritative section processing	470
Additional section processing	470
Resolving DNS queries between VPCs and your network	471
How DNS resolvers on your network forward DNS queries to Route 53 Resolver endpoints	473
How Route 53 Resolver endpoint forwards DNS queries from your VPCs to your network	473
Using rules to control which queries are forwarded to your network	474
How Resolver determines whether the domain name in a query matches any rules	476
How Resolver determines where to forward DNS queries	476
Using rules in multiple Regions	477
Domain names that Resolver creates autodefined system rules for	477
Considerations when creating inbound and outbound endpoints	478
Getting started with Route 53 Resolver	480
Forwarding inbound DNS queries to your VPCs	481
Configuring inbound forwarding	481
Values that you specify when you create or edit inbound endpoints	482
Forwarding outbound DNS queries to your network	483
Configuring outbound forwarding	483
Values that you specify when you create or edit outbound endpoints	484
Values that you specify when you create or edit rules	485
Managing inbound endpoints	486
Viewing and editing inbound endpoints	487
Viewing the status for inbound endpoints	487
Deleting inbound endpoints	488
Managing outbound endpoints	488
Viewing and editing outbound endpoints	488
Viewing the status for outbound endpoints	489
Deleting outbound endpoints	489
Managing forwarding rules	490
Viewing and editing forwarding rules	490
Creating forwarding rules	491
Adding rules for reverse lookup	491
Associating forwarding rules with a VPC	491
Disassociating forwarding rules from a VPC	492
Sharing forwarding rules with other AWS accounts and using shared rules	492
Deleting forwarding rules	494

Forwarding rules for reverse DNS queries in Resolver	495
Enabling DNSSEC validation	495
Routing internet traffic to your AWS resources	496
Amazon API Gateway API	496
Prerequisites	496
Configuring Route 53 to route traffic to an API Gateway endpoint	497
Amazon CloudFront distribution	498
Prerequisites	499
Configuring Amazon Route 53 to route traffic to a CloudFront distribution	499
Amazon EC2 instance	500
Prerequisites	501
Configuring Amazon Route 53 to route traffic to an Amazon EC2 instance	501
AWS Elastic Beanstalk environment	502
Deploying an application into an Elastic Beanstalk environment	503
Getting the domain name for your Elastic Beanstalk environment	503
Creating a Route 53 record	503
ELB load balancer	505
Prerequisites	506
Configuring Amazon Route 53 to route traffic to an ELB load balancer	506
Amazon S3 bucket	507
Prerequisites	508
Configuring Amazon Route 53 to route traffic to an S3 Bucket	508
Amazon Virtual Private Cloud interface endpoint	509
Prerequisites	510
Amazon VPC interface endpoint	510
Amazon WorkMail	511
Other AWS resources	513
AWS CloudFormation resources	513
Route 53, Route 53 Resolver, and AWS CloudFormation templates	513
Learn more about AWS CloudFormation	514
Creating health checks and configuring DNS failover	515
Types of health checks	516
How Route 53 determines whether a health check is healthy	516
How Route 53 determines the status of health checks that monitor an endpoint	517
How Route 53 determines the status of health checks that monitor other health checks	518
How Route 53 determines the status of health checks that monitor CloudWatch alarms	518
Creating, updating, and deleting health checks	518
Creating and updating health checks	519
Values that you specify when you create or update health checks	519
Values that Route 53 displays when you create a health check	528
Updating health checks when you change CloudWatch alarm settings	528
Deleting health checks	528
Updating or deleting health checks when DNS failover is configured	529
Configuring router and firewall rules for health checks	529
Monitoring health check status and getting notifications	530
Viewing health check status and the reason for health check failures	530
Monitoring the latency between health checkers and your endpoint	531
Monitoring health checks using CloudWatch	532
Configuring DNS failover	536
Task list for configuring DNS failover	537
How health checks work in simple configurations	538
How health checks work in complex configurations	541
How Route 53 chooses records when health checking is configured	546
Active-active and active-passive failover	547
Configuring failover in a private hosted zone	550
How Route 53 averts failover problems	550
Naming and tagging health checks	551

Tag restrictions	551
Adding, editing, and deleting tags for health checks	552
Using API versions before 2012-12-12	553
Route 53 Resolver DNS Firewall	554
How Route 53 Resolver DNS Firewall works	554
DNS Firewall components and settings	555
How Route 53 Resolver DNS Firewall filters DNS queries	556
High-level steps for using DNS Firewall	556
Using DNS Firewall rule groups in multiple Regions	557
Getting started with Route 53 Resolver DNS Firewall	557
Route 53 Resolver DNS Firewall walled garden example	557
Route 53 Resolver DNS Firewall block list example	559
DNS Firewall rule groups and rules	560
Rule group settings in DNS Firewall	560
Rule settings in DNS Firewall	561
Rule actions in DNS Firewall	561
Managing rule groups and rules in DNS Firewall	562
Route 53 Resolver DNS Firewall domain lists	563
Managed domain lists	564
Managing your own domain lists	566
Configuring query logging for DNS Firewall	567
Sharing rule groups between accounts	568
Enabling DNS Firewall protections for your VPC	570
Managing associations between your VPC and firewall rule groups	570
DNS Firewall VPC configuration	571
Security	573
Data protection	573
Protection from dangling delegation records	574
Identity and access management	574
Authentication	574
Access control	575
Overview of managing access	576
Using IAM policies for Route 53	579
Using Service-Linked Roles	587
AWS managed policies	590
Route 53 API permissions reference	595
Logging and monitoring	612
Compliance validation	613
Resilience	613
Infrastructure security	614
Monitoring	615
Public DNS query logging	615
Configuring logging for DNS queries	616
Using Amazon CloudWatch to access DNS query logs	617
Changing the retention period for logs and exporting logs to Amazon S3	617
Stopping query logging	617
Values that appear in DNS query logs	618
Query log example	619
Resolver query logging	619
Resources that you can send Resolver query logs to	620
Managing configurations	621
Monitoring domain registrations	626
Monitoring your resources with Amazon Route 53 health checks and Amazon CloudWatch	626
Metrics and dimensions for health checks	627
Monitoring hosted zones using Amazon CloudWatch	628
CloudWatch metric for Route 53 public hosted zones	629
CloudWatch dimension for Route 53 public hosted zone metrics	630

Monitoring Route 53 Resolver endpoints with Amazon CloudWatch	630
Metrics and dimensions for Resolver	630
Monitoring Route 53 Resolver DNS Firewall rule groups with Amazon CloudWatch	633
Metrics and dimensions for DNS Firewall	633
Logging Amazon Route 53 API calls with AWS CloudTrail	635
Route 53 information in CloudTrail	635
Viewing Route 53 events in event history	636
Understanding Route 53 log file entries	636
Troubleshooting	642
My domain is unavailable on the internet	642
You registered a new domain, but you didn't click the link in the confirmation email	642
You transferred domain registration to Amazon Route 53, but you didn't transfer DNS service ...	643
You transferred domain registration and specified the wrong name servers in the domain settings	643
You transferred DNS service first, but you didn't wait long enough before transferring domain registration	644
You deleted the hosted zone that Route 53 is using to route internet traffic for the domain	645
Your domain has been suspended	645
My domain is suspended (status is ClientHold)	646
You registered a new domain, but you didn't click the link in the confirmation email	646
You disabled automatic renewal for the domain, and the domain expired	647
You changed the email address for the registrant contact, but you didn't verify that the new email address is valid	647
We couldn't process your payment for automatic domain renewal, and the domain expired	647
We suspended the domain for a violation of the AWS Acceptable Use Policy	647
We suspended the domain because of a court order	648
Transferring my domain to Amazon Route 53 failed	648
You didn't click the link in the authorization email	648
The authorization code that you got from the current registrar is not valid	648
"Parameters in request are not valid" error when trying to transfer a .es domain to Amazon Route 53	649
I changed DNS settings, but they haven't taken effect	649
You transferred DNS service to Amazon Route 53 in the last 48 hours, so DNS is still using your previous DNS service	649
You recently transferred DNS service to Amazon Route 53, but you didn't update the name servers with the domain registrar	649
DNS resolvers still are using the old settings for the record	650
You have more than one hosted zone with the same name, and you updated the one that isn't associated with the domain	651
My browser displays a "Server not found" error	652
You didn't create a record for the domain or subdomain name	652
You created a record but specified the wrong value	652
The resource that you're routing traffic to is unavailable	652
I can't route traffic to an Amazon S3 bucket that's configured for website hosting	652
I was billed twice for the same hosted zone	653
My AWS account is closed, suspended, or terminated, and my domain is registered with Route 53	653
IP address ranges	654
Tagging resources	655
Tutorials	656
Using Amazon Route 53 as the DNS service for subdomains without migrating the parent domain	656
Creating a subdomain that uses Amazon Route 53 as the DNS service without migrating the parent domain	656
Migrating DNS service for a subdomain to Amazon Route 53 without migrating the parent domain	658
Transitioning to latency-based routing in Amazon Route 53	661
Adding another Region to your latency-based routing in Amazon Route 53	662

Using latency and weighted records in Amazon Route 53 to route traffic to multiple Amazon EC2 instances in a Region	664
Managing over 100 weighted records in Amazon Route 53	664
Weighting fault-tolerant multi-record answers in Amazon Route 53	665
Best practices	667
Best practices for Amazon Route 53 DNS	667
Best practices for Resolver	668
Avoid loop configurations with Resolver endpoints	669
Resolver endpoint scaling	669
High availability for Resolver endpoints	669
DNS zone walking	670
Best practices for Amazon Route 53 health checks	670
Best practices for Elastic IP addresses for health checks	670
Quotas	671
Using Service Quotas to view and manage quotas	671
Quotas on entities	671
Quotas on domains	672
Quotas on hosted zones	672
Quotas on records	672
Quotas on Route 53 Resolver	673
Quotas on health checks	675
Quotas on query log configurations	675
Quotas on traffic flow policies and policy records	675
Quotas on reusable delegation sets	675
Maximums on API requests	675
Number of elements and characters in ChangeResourceRecordSets requests	676
Frequency of Amazon Route 53 API requests	676
Frequency of Route 53 Resolver API requests	676
Related information	678
AWS resources	678
Third-party tools and libraries	679
Graphical user interfaces	679
Document history	681
2022 releases	681
2021 releases	681
2020 releases	682
2018 releases	682
2017 releases	683
2016 releases	684
2015 releases	686
2014 releases	688
2013 releases	690
2012 release	691
2011 releases	691
2010 release	691
AWS glossary	692

What is Amazon Route 53?

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. You can use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking.

If you choose to use Route 53 for all three functions, be sure to follow the order below:

1. Register domain names

Your website needs a name, such as example.com. Route 53 lets you register a name for your website or web application, known as a *domain name*.

- For an overview, see [How domain registration works \(p. 1\)](#).
- For a procedure, see [Registering a new domain \(p. 42\)](#).
- For a tutorial that takes you through registering a domain and creating a simple website in an Amazon S3 bucket, see [Getting started with Amazon Route 53 \(p. 17\)](#).

2. Route internet traffic to the resources for your domain

When a user opens a web browser and enters your domain name (example.com) or subdomain name (acme.example.com) in the address bar, Route 53 helps connect the browser with your website or web application.

- For an overview, see [How internet traffic is routed to your website or web application \(p. 2\)](#).
- For procedures, see [Configuring Amazon Route 53 as your DNS service \(p. 325\)](#).
- For a procedure on how to route email to Amazon WorkMail, see [Routing traffic to Amazon WorkMail \(p. 511\)](#).

3. Check the health of your resources

Route 53 sends automated requests over the internet to a resource, such as a web server, to verify that it's reachable, available, and functional. You also can choose to receive notifications when a resource becomes unavailable and choose to route internet traffic away from unhealthy resources.

- For an overview, see [How Amazon Route 53 checks the health of your resources \(p. 5\)](#).
- For procedures, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

Topics

- [How domain registration works \(p. 1\)](#)
- [How internet traffic is routed to your website or web application \(p. 2\)](#)
- [How Amazon Route 53 checks the health of your resources \(p. 5\)](#)
- [Amazon Route 53 concepts \(p. 6\)](#)
- [How to get started with Amazon Route 53 \(p. 11\)](#)
- [Related services \(p. 11\)](#)
- [Accessing Amazon Route 53 \(p. 11\)](#)
- [AWS Identity and Access Management \(p. 12\)](#)
- [Amazon Route 53 pricing and billing \(p. 12\)](#)

How domain registration works

If you want to create a website or a web application, you start by registering the name of your website, known as a *domain name*. Your domain name is the name, such as example.com, that your users enter in a browser to display your website.

Here's an overview of how you register a domain name with Amazon Route 53:

1. You choose a domain name and confirm that it's available, meaning that no one else has registered the domain name that you want.

If the domain name you want is already in use, you can try other names or try changing only the *top-level domain*, such as .com, to another top-level domain, such as .ninja or .hockey. For a list of the top-level domains that Route 53 supports, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

2. You register the domain name with Route 53. When you register a domain, you provide names and contact information for the domain owner and other contacts.

When you register a domain with Route 53, the service automatically makes itself the DNS service for the domain by doing the following:

- Creates a [hosted zone](#) that has the same name as your domain.
- Assigns a set of four name servers to the hosted zone. When someone uses a browser to access your website, such as www.example.com, these name servers tell the browser where to find your resources, such as a web server or an Amazon S3 bucket. ([Amazon S3](#) is object storage for storing and retrieving any amount of data from anywhere on the web. A bucket is a container for objects that you store in S3.)
- Gets the name servers from the hosted zone and adds them to the domain.

For more information, see [How internet traffic is routed to your website or web application \(p. 2\)](#).

3. At the end of the registration process, we send your information to the registrar for the domain. The [domain registrar](#) is either Amazon Registrar, Inc. or our registrar associate, Gandi. To find out who the registrar is for your domain, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).
4. The registrar sends your information to the *registry* for the domain. A registry is a company that sells domain registrations for one or more top-level domains, such as .com.
5. The registry stores the information about your domain in their own database and also stores some of the information in the public WHOIS database.

For more information about how to register a domain name, see [Registering a new domain \(p. 42\)](#).

If you already registered a domain name with another registrar, you can choose to transfer the domain registration to Route 53. This isn't required to use other Route 53 features. For more information, see [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#).

How internet traffic is routed to your website or web application

All computers on the internet, from your smart phone or laptop to the servers that serve content for massive retail websites, communicate with one another by using numbers. These numbers, known as *IP addresses*, are in one of the following formats:

- Internet Protocol version 4 (IPv4) format, such as 192.0.2.44
- Internet Protocol version 6 (IPv6) format, such as 2001:0db8:85a3:0000:0000:abcd:0001:2345

When you open a browser and go to a website, you don't have to remember and enter a long string of characters like that. Instead, you can enter a domain name like example.com and still end up in the right place. A DNS service such as Amazon Route 53 helps to make that connection between domain names and IP addresses.

Topics

- [Overview of how you configure Amazon Route 53 to route internet traffic for your domain \(p. 3\)](#)
- [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#)

Overview of how you configure Amazon Route 53 to route internet traffic for your domain

Here's an overview of how to use the Amazon Route 53 console to register a domain name and configure Route 53 to route internet traffic to your website or web application.

1. You register the domain name that you want your users to use to access your content. For an overview, see [How domain registration works \(p. 1\)](#).
2. After you register your domain name, Route 53 automatically creates a public hosted zone that has the same name as the domain. For more information, see [Working with public hosted zones \(p. 339\)](#).
3. To route traffic to your resources, you create *records*, also known as *resource record sets*, in your hosted zone. Each record includes information about how you want to route traffic for your domain, such as the following:

Name

The name of the record corresponds with the domain name (example.com) or subdomain name (www.example.com, retail.example.com) that you want Route 53 to route traffic for.

The name of every record in a hosted zone must end with the name of the hosted zone. For example, if the name of the hosted zone is example.com, all record names must end in example.com. The Route 53 console does this for you automatically.

Type

The record type usually determines the type of resource that you want traffic to be routed to. For example, to route traffic to an email server, you specify MX for Type. To route traffic to a web server that has an IPv4 IP address, you specify A for Type.

Value

Value is closely related to Type. If you specify MX for Type, you specify the names of one or more email servers for Value. If you specify A for Type, you specify an IP address in IPv4 format, such as 192.0.2.136.

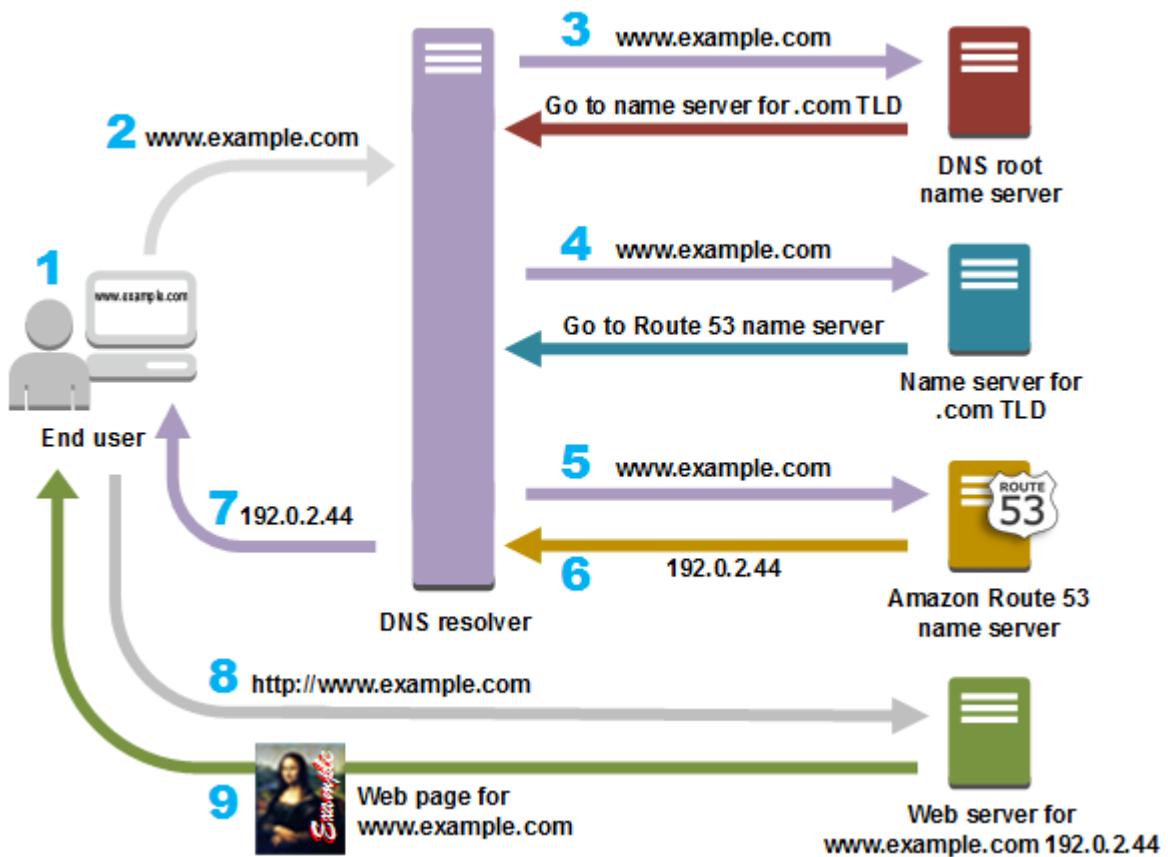
For more information about records, see [Working with records \(p. 370\)](#).

You can also create special Route 53 records, called alias records, that route traffic to Amazon S3 buckets, Amazon CloudFront distributions, and other AWS resources. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#) and [Routing internet traffic to your AWS resources \(p. 496\)](#).

For more information about routing internet traffic to your resources, see [Configuring Amazon Route 53 as your DNS service \(p. 325\)](#).

How Amazon Route 53 routes traffic for your domain

After you configure Amazon Route 53 to route your internet traffic to your resources, such as web servers or Amazon S3 buckets, here's what happens in just a few milliseconds when someone requests content for www.example.com:



1. A user opens a web browser, enters www.example.com in the address bar, and presses Enter.
2. The request for www.example.com is routed to a DNS resolver, which is typically managed by the user's internet service provider (ISP), such as a cable internet provider, a DSL broadband provider, or a corporate network.
3. The DNS resolver for the ISP forwards the request for www.example.com to a DNS root name server.
4. The DNS resolver forwards the request for www.example.com again, this time to one of the TLD name servers for .com domains. The name server for .com domains responds to the request with the names of the four Route 53 name servers that are associated with the example.com domain.

The DNS resolver caches (stores) the four Route 53 name servers. The next time someone browses to example.com, the resolver skips steps 3 and 4 because it already has the name servers for example.com. The name servers are typically cached for two days.

5. The DNS resolver chooses a Route 53 name server and forwards the request for www.example.com to that name server.
6. The Route 53 name server looks in the example.com hosted zone for the www.example.com record, gets the associated value, such as the IP address for a web server, 192.0.2.44, and returns the IP address to the DNS resolver.
7. The DNS resolver finally has the IP address that the user needs. The resolver returns that value to the web browser.

Note

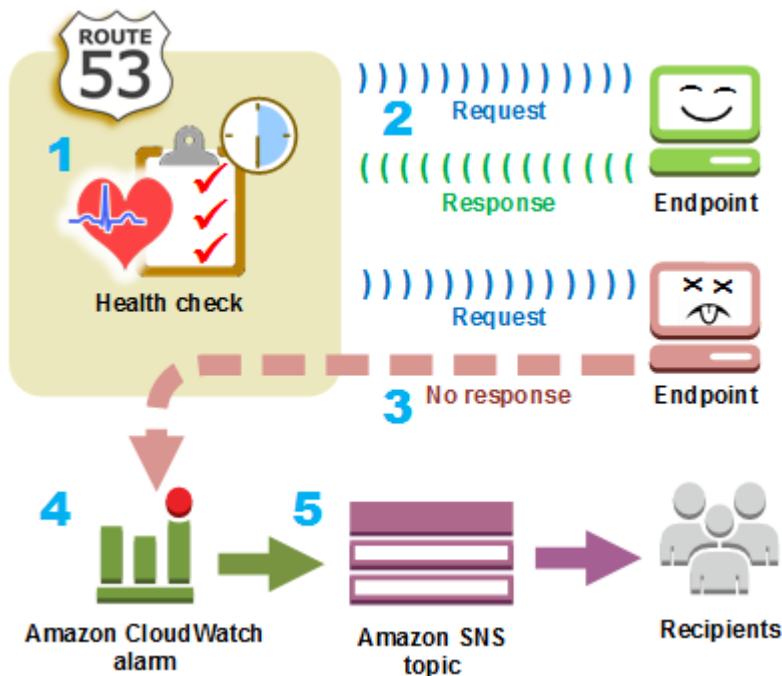
The DNS resolver also caches the IP address for example.com for an amount of time that you specify so that it can respond more quickly the next time someone browses to example.com. For more information, see [time to live \(TTL\)](#).

8. The web browser sends a request for `www.example.com` to the IP address that it got from the DNS resolver. This is where your content is, for example, a web server running on an Amazon EC2 instance or an Amazon S3 bucket that's configured as a website endpoint.
9. The web server or other resource at `192.0.2.44` returns the web page for `www.example.com` to the web browser, and the web browser displays the page.

How Amazon Route 53 checks the health of your resources

Amazon Route 53 health checks monitor the health of your resources such as web servers and email servers. You can optionally configure Amazon CloudWatch alarms for your health checks, so that you receive notification when a resource becomes unavailable.

Here's an overview of how health checking works if you want to be notified when a resource becomes unavailable:



1. You create a health check and specify values that define how you want the health check to work, such as the following:
 - The IP address or domain name of the endpoint, such as a web server, that you want Route 53 to monitor. (You can also monitor the status of other health checks, or the state of a CloudWatch alarm.)
 - The protocol that you want Amazon Route 53 to use to perform the check: HTTP, HTTPS, or TCP.
 - How often you want Route 53 to send a request to the endpoint. This is the *request interval*.
 - How many consecutive times the endpoint must fail to respond to requests before Route 53 considers it unhealthy. This is the *failure threshold*.
 - Optionally, how you want to be notified when Route 53 detects that the endpoint is unhealthy. When you configure notification, Route 53 automatically sets a CloudWatch alarm. CloudWatch uses Amazon SNS to notify users that an endpoint is unhealthy.
2. Route 53 starts to send requests to the endpoint at the interval that you specified in the health check.

If the endpoint responds to the requests, Route 53 considers the endpoint to be healthy and takes no action.

3. If the endpoint doesn't respond to a request, Route 53 starts to count the number of consecutive requests that the endpoint doesn't respond to:
 - If the count reaches the value that you specified for the failure threshold, Route 53 considers the endpoint unhealthy.
 - If the endpoint starts to respond again before the count reaches the failure threshold, Route 53 resets the count to 0, and CloudWatch doesn't contact you.
4. If Route 53 considers the endpoint unhealthy and if you configured notification for the health check, Route 53 notifies CloudWatch.

If you didn't configure notification, you can still see the status of your Route 53 health checks in the Route 53 console. For more information, see [Monitoring health check status and getting notifications \(p. 530\)](#).

5. If you configured notification for the health check, CloudWatch triggers an alarm and uses Amazon SNS to send notification to the specified recipients.

In addition to checking the health of a specified endpoint, you can configure a health check to check the health of one or more other health checks so that you can be notified when a specified number of resources, such as two web servers out of five, are unavailable. You can also configure a health check to check the status of a CloudWatch alarm so that you can be notified on the basis of a broad range of criteria, not just whether a resource is responding to requests.

If you have multiple resources that perform the same function, for example, web servers or database servers, and you want Route 53 to route traffic only to the resources that are healthy, you can configure DNS failover by associating a health check with each record for that resource. If a health check determines that the underlying resource is unhealthy, Route 53 routes traffic away from the associated record.

For more information about using Route 53 to monitor the health of your resources, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

Amazon Route 53 concepts

Here's an overview of the concepts that are discussed throughout the *Amazon Route 53 Developer Guide*.

Topics

- [Domain registration concepts \(p. 6\)](#)
- [Domain Name System \(DNS\) concepts \(p. 7\)](#)
- [Health checking concepts \(p. 10\)](#)

Domain registration concepts

Here's an overview of the concepts that are related to domain registration.

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

domain name

The name, such as example.com, that a user types in the address bar of a web browser to access a website or a web application. To make your website or web application available on the internet, you start by registering a domain name. For more information, see [How domain registration works \(p. 1\)](#).

domain registrar

A company that is accredited by ICANN (Internet Corporation for Assigned Names and Numbers) to process domain registrations for specific top-level domains (TLDs). For example, Amazon Registrar, Inc. is a domain registrar for .com, .net, and .org domains. Our registrar associate, Gandi, is a domain registrar for hundreds of TLDs, such as .apartments, .boutique, and .camera. For more information, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

domain registry

A company that owns the right to sell domains that have a specific top-level domain. For example, [VeriSign](#) is the registry that owns the right to sell domains that have a .com TLD. A domain registry defines the rules for registering a domain, such as residency requirements for a geographic TLD. A domain registry also maintains the authoritative database for all of the domain names that have the same TLD. The registry's database contains information such as contact information and the name servers for each domain.

domain reseller

A company that sells domain names for registrars such as Amazon Registrar. Amazon Route 53 is a domain reseller for Amazon Registrar and for our registrar associate, Gandi.

top-level domain (TLD)

The last part of a domain name, such as .com, .org, or .ninja. There are two types of top-level domains:

Generic top-level domains

These TLDs typically give users an idea of what they'll find on the website. For example, domain names that have a TLD of *.bike* often are associated with websites for motorcycle or bicycle businesses or organizations. With a few exceptions, you can use any generic TLD you want, so a bicycle club could use the *.hockey* TLD for their domain name.

Geographic top-level domains

These TLDs are associated with geographic areas such as countries or cities. Some registries for geographic TLDs have residency requirements, while others, such as [the section called ".io \(British Indian Ocean Territory\)" \(p. 300\)](#), allow or even encourage use as a generic TLD.

For a list of the TLDs that you can use when you register a domain name with Route 53, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Domain Name System (DNS) concepts

Here's an overview of the concepts that are related to the Domain Name System (DNS).

- [alias record](#)
- [authoritative name server](#)
- [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)

alias record

A type of record that you can create with Amazon Route 53 to route traffic to AWS resources such as Amazon CloudFront distributions and Amazon S3 buckets. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

authoritative name server

A name server that has definitive information about one part of the Domain Name System (DNS) and that responds to requests from a DNS resolver by returning the applicable information. For example, an authoritative name server for the .com top-level domain (TLD) knows the names of the name servers for every registered .com domain. When a .com authoritative name server receives a request from a DNS resolver for example.com, it responds with the names of the name servers for the DNS service for the example.com domain.

Route 53 name servers are the authoritative name servers for every domain that uses Route 53 as the DNS service. The name servers know how you want to route traffic for your domain and subdomains based on the records that you created in the hosted zone for the domain. (Route 53 name servers store the hosted zones for the domains that use Route 53 as the DNS service.)

For example, if a Route 53 name server receives a request for www.example.com, it finds that record and returns the IP address, such as 192.0.2.33, that is specified in the record.

DNS query

Usually a request that is submitted by a device, such as a computer or a smart phone, to the Domain Name System (DNS) for a resource that is associated with a domain name. The most common example of a DNS query is when a user opens a browser and types the domain name in the address bar. The response to a DNS query typically is the IP address that is associated with a resource such as a web server. The device that initiated the request uses the IP address to communicate with the resource. For example, a browser can use the IP address to get a web page from a web server.

DNS resolver

A DNS server, often managed by an internet service provider (ISP), that acts as an intermediary between user requests and DNS name servers. When you open a browser and enter a domain name in the address bar, your query goes first to a DNS resolver. The resolver communicates with DNS name servers to get the IP address for the corresponding resource, such as a web server. A DNS resolver is also known as a recursive name server because it sends requests to a sequence of authoritative DNS name servers until it gets the response (typically an IP address) that it returns to a user's device, for example, a web browser on a laptop computer.

Domain Name System (DNS)

A worldwide network of servers that help computers, smart phones, tablets, and other IP-enabled devices to communicate with one another. The Domain Name System translates easily understood names such as example.com into the numbers, known as *IP addresses*, that allow computers to find each other on the internet.

See also [IP address](#).

hosted zone

A container for records, which include information about how you want to route traffic for a domain (such as example.com) and all of its subdomains (such as www.example.com, retail.example.com, and seattle.accounting.example.com). A hosted zone has the same name as the corresponding domain.

For example, the hosted zone for example.com might include a record that has information about routing traffic for www.example.com to a web server that has the IP address 192.0.2.243, and a record that has information about routing email for example.com to two email servers, mail1.example.com and mail2.example.com. Each email server also requires its own record.

See also [record \(DNS record\)](#).

IP address

A number that is assigned to a device on the internet—such as a laptop, a smart phone, or a web server—that allows the device to communicate with other devices on the internet. IP addresses are in one of the following formats:

- Internet Protocol version 4 (IPv4) format, such as 192.0.2.44
- Internet Protocol version 6 (IPv6) format, such as 2001:0db8:85a3:0000:0000:abcd:0001:2345

Route 53 supports both IPv4 and IPv6 addresses for the following purposes:

- You can create records that have a type of A, for IPv4 addresses, or a type of AAAA, for IPv6 addresses.
- You can create health checks that send requests either to IPv4 or to IPv6 addresses.
- If a DNS resolver is on an IPv6 network, it can use either IPv4 or IPv6 to submit requests to Route 53.

name servers

Servers in the Domain Name System (DNS) that help to translate domain names into the IP addresses that computers use to communicate with one another. Name servers are either recursive name servers (also known as [DNS resolver](#)) or [authoritative name servers](#).

For an overview of how DNS routes traffic to your resources, including the role of Route 53 in the process, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

private DNS

A local version of the Domain Name System (DNS) that lets you route traffic for a domain and its subdomains to Amazon EC2 instances within one or more Amazon virtual private clouds (VPCs). For more information, see [Working with private hosted zones \(p. 356\)](#).

record (DNS record)

An object in a hosted zone that you use to define how you want to route traffic for the domain or a subdomain. For example, you might create records for example.com and www.example.com that route traffic to a web server that has an IP address of 192.0.2.234.

For more information about records, including information about functionality that is provided by Route 53-specific records, see [Configuring Amazon Route 53 as your DNS service \(p. 325\)](#).

recursive name server

See [DNS resolver](#).

reusable delegation set

A set of four authoritative name servers that you can use with more than one hosted zone. By default, Route 53 assigns a random selection of name servers to each new hosted zone. To make it

easier to migrate DNS service to Route 53 for a large number of domains, you can create a reusable delegation set and then associate the reusable delegation set with new hosted zones. (You can't change the name servers that are associated with an existing hosted zone.)

You create a reusable delegation set and associate it with a hosted zone programmatically; using the Route 53 console isn't supported. For more information, see [CreateHostedZone](#) and [CreateReusableDelegationSet](#) in the *Amazon Route 53 API Reference*. The same feature is also available in the [AWS SDKs](#), the [AWS Command Line Interface](#), and [AWS Tools for Windows PowerShell](#).

routing policy

A setting for records that determines how Route 53 responds to DNS queries. Route 53 supports the following routing policies:

- **Simple routing policy** – Use to route internet traffic to a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route internet traffic to your resources based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple locations and you want to route traffic to the resource that provides the best latency.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

For more information, see [Choosing a routing policy \(p. 371\)](#).

subdomain

A domain name that has one or more labels prepended to the registered domain name. For example, if you register the domain name example.com, then www.example.com is a subdomain. If you create the hosted zone accounting.example.com for the example.com domain, then seattle.accounting.example.com is a subdomain.

To route traffic for a subdomain, create a record that has the name that you want, such as www.example.com, and specify the applicable values, such as the IP address of a web server.

time to live (TTL)

The amount of time, in seconds, that you want a DNS resolver to cache (store) the values for a record before submitting another request to Route 53 to get the current values for that record. If the DNS resolver receives another request for the same domain before the TTL expires, the resolver returns the cached value.

A longer TTL reduces your Route 53 charges, which are based in part on the number of DNS queries that Route 53 responds to. A shorter TTL reduces the amount of time that DNS resolvers route traffic to older resources after you change the values in a record, for example, by changing the IP address for the web server for www.example.com.

Health checking concepts

Here's an overview of the concepts that are related to Amazon Route 53 health checking.

- [DNS failover](#)

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

DNS failover

A method for routing traffic away from unhealthy resources and to healthy resources. When you have more than one resource performing the same function—for example, more than one web server or mail server—you can configure Route 53 health checks to check the health of your resources and configure records in your hosted zone to route traffic only to healthy resources.

For more information, see [Configuring DNS failover \(p. 536\)](#).

endpoint

The resource, such as a web server or an email server, that you configure a health check to monitor the health of. You can specify an endpoint by IPv4 address (192.0.2.243), by IPv6 address (2001:0db8:85a3:0000:0000:abcd:0001:2345), or by domain name (example.com).

Note

You can also create health checks that monitor the status of other health checks or that monitor the alarm state of a CloudWatch alarm.

health check

A Route 53 component that lets you do the following:

- Monitor whether a specified endpoint, such as a web server, is healthy
- Optionally, get notified when an endpoint becomes unhealthy
- Optionally, configure DNS failover, which allows you to reroute internet traffic from an unhealthy resource to a healthy resource

For more information about how to create and use health checks, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

How to get started with Amazon Route 53

For information about getting started with Amazon Route 53, see the following topics in this guide:

- [Setting up Amazon Route 53 \(p. 13\)](#), which explains how to sign up for AWS, how to secure access to your AWS account, and how to set up programmatic access to Route 53
- [Getting started with Amazon Route 53 \(p. 17\)](#), which describes how to register a domain name, how to create an Amazon S3 bucket and configure it to host a static website, and how to route internet traffic to the website

Related services

For information about the AWS services that Amazon Route 53 integrates with, see [Integration with other services \(p. 35\)](#).

Accessing Amazon Route 53

You can access Amazon Route 53 in the following ways:

- **AWS Management Console** – The procedures throughout this guide explain how to use the AWS Management Console to perform tasks.
- **AWS SDKs** – If you're using a programming language that AWS provides an SDK for, you can use an SDK to access Route 53. SDKs simplify authentication, integrate easily with your development environment, and provide easy access to Route 53 commands. For more information, see [Tools for Amazon Web Services](#).
- **Route 53 API** – If you're using a programming language that an SDK isn't available for, see the [Amazon Route 53 API Reference](#) for information about API actions and about how to make API requests.
- **AWS Command Line Interface** – For more information, see [Getting set up with the AWS Command Line Interface](#) in the [AWS Command Line Interface User Guide](#).
- **AWS Tools for Windows PowerShell** – For more information, see [Setting up the AWS Tools for Windows PowerShell](#) in the [AWS Tools for Windows PowerShell User Guide](#).

AWS Identity and Access Management

Amazon Route 53 integrates with AWS Identity and Access Management (IAM), a service that lets your organization do the following:

- Create users and groups under your organization's AWS account
- Easily share your AWS account resources among the users in the account
- Assign unique security credentials to each user
- Granularly control user access to services and resources

For example, you can use IAM with Route 53 to control which users in your AWS account can create a new hosted zone or change records.

For general information about IAM, see the following:

- [Identity and access management in Amazon Route 53 \(p. 574\)](#)
- [Identity and Access Management \(IAM\)](#)
- [IAM User Guide](#)

Amazon Route 53 pricing and billing

As with other AWS products, there are no contracts or minimum commitments for using Amazon Route 53. You pay only for the hosted zones that you configure and the number of DNS queries that Route 53 answers. For more information, see [Amazon Route 53 Pricing](#).

For information about billing for AWS services, including how to view your bill and manage your account and payments, see the [AWS Billing and Cost Management User Guide](#).

Setting up Amazon Route 53

The overview and procedures in this section help you get started with AWS.

Topics

- [Sign up for AWS \(p. 13\)](#)
- [Access your account \(p. 13\)](#)
- [Create an IAM user \(p. 14\)](#)
- [Set up the AWS Command Line Interface or AWS Tools for Windows PowerShell \(p. 15\)](#)
- [Download an AWS SDK \(p. 16\)](#)

Sign up for AWS

When you sign up for AWS, your AWS account is automatically signed up for all services in AWS, including Amazon Route 53. You are charged only for the services that you use.

If you have an AWS account already, skip to [Access your account \(p. 13\)](#). If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Note your AWS account number, because you'll need it later.

Access your account

You use AWS services by using any of the following options:

- AWS Management Console
- API for each service
- AWS Command Line Interface (AWS CLI)
- AWS Tools for Windows PowerShell
- AWS SDKs

For each of those options, you need to access your AWS account by providing credentials that verify that you have permissions to use the services.

Access the console

To access the AWS Management Console for the first time, you provide an email address and a password. This combination of your email address and password is called your *root identity* or *root account credentials*. After you access your account for the first time, we strongly recommend that you don't use

your root account credentials again for everyday use. Instead, you should create new credentials by using [AWS Identity and Access Management](#). To do that, you create a user account for yourself known as an *IAM user*, and then add the IAM user to an IAM group with administrative permissions or grant the IAM user administrative permissions. You then can access AWS using a special URL and the credentials for the IAM user. You also can add other IAM users later, and restrict their access to specified resources in the account.

Access the API, AWS CLI, AWS Tools for Windows PowerShell, or the AWS SDKs

To use the API, the AWS CLI, AWS Tools for Windows PowerShell, or the AWS SDKs, you must create *access keys*. These keys consist of an access key ID and secret access key, which are used to sign programmatic requests that you make to AWS.

To create the keys, you sign in to the AWS Management Console. We strongly recommend that you sign in with your IAM user credentials instead of your root credentials. For more information, see [Managing access keys for IAM users](#) in the *IAM User Guide*.

Create an IAM user

Perform the following procedures to create a group for administrators, create an IAM user, and then add the IAM user to the administrators group. If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console. If you aren't familiar with using the console, see [Working with the AWS Management Console](#) for an overview.

To create an administrator user for yourself and add the user to an administrators group (console)

1. Sign in to the [IAM console](#) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

Note

We strongly recommend that you adhere to the best practice of using the **Administrator** IAM user that follows and securely lock away the root user credentials. Sign in as the root user only to perform a few [account and service management tasks](#).

2. In the navigation pane, choose **Users** and then choose **Add user**.
3. For **User name**, enter **Administrator**.
4. Select the check box next to **AWS Management Console access**. Then select **Custom password**, and then enter your new password in the text box.
5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to **User must create a new password at next sign-in** to allow the new user to reset their password after they sign in.
6. Choose **Next: Permissions**.
7. Under **Set permissions**, choose **Add user to group**.
8. Choose **Create group**.
9. In the **Create group** dialog box, for **Group name** enter **Administrators**.
10. Choose **Filter policies**, and then select **AWS managed - job function** to filter the table contents.
11. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.

Note

You must activate IAM user and role access to Billing before you can use the **AdministratorAccess** permissions to access the AWS Billing and Cost Management

console. To do this, follow the instructions in [step 1 of the tutorial about delegating access to the billing console](#).

12. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
13. Choose **Next: Tags**.
14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see [Tagging IAM entities](#) in the *IAM User Guide*.
15. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see [Access management](#) and [Example policies](#).

To sign in as your new IAM user

1. Sign out of the AWS console.
2. Sign in by using the following URL, where *your_aws_account_id* is your AWS account number without the hyphens. For example, if your AWS account number is 1234-5678-9012, your AWS account ID is 123456789012:

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

3. Enter the IAM user name (not your email address) and password that you just created. When you're signed in, the navigation bar displays "*your_user_name* @ *your_aws_account_id*".

If you don't want the URL for your sign-in page to contain your AWS account ID, you can create an account alias.

To create an account alias and conceal your account ID

1. On the IAM console, choose **Dashboard** in the navigation pane.
2. On the dashboard, choose **Customize** and enter an alias such as your company name.
3. Sign out of the AWS console.
4. Sign in by using the following URL:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

To verify the sign-in link for IAM users for your account, open the IAM console and check under **IAM users sign-in link** on the dashboard.

For more information about using IAM, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Set up the AWS Command Line Interface or AWS Tools for Windows PowerShell

The AWS Command Line Interface (AWS CLI) is a unified tool for managing AWS services. For information about how to install and configure the AWS CLI, see [Getting set up with the AWS Command Line Interface](#) in the *AWS Command Line Interface User Guide*.

If you have experience with Windows PowerShell, you might prefer to use AWS Tools for Windows PowerShell. For more information, see [Setting up the AWS Tools for Windows PowerShell](#) in the [AWS Tools for Windows PowerShell User Guide](#).

Download an AWS SDK

If you're using a programming language that AWS provides an SDK for, we recommend that you use an SDK instead of the Amazon Route 53 API. The SDKs make authentication simpler, integrate easily with your development environment, and provide easy access to Route 53 commands. For more information, see [Tools for Amazon Web Services](#).

Getting started with Amazon Route 53

Get started with the basic steps by registering a domain with Amazon Route 53 and configuring Route 53 to respond to DNS queries that resolve to a static website. The first tutorial hosts a static website in an open Amazon S3 bucket, and the second tutorial uses Amazon CloudFront distribution to serve the website with SSL/TLS.

Estimated cost

- There's an annual fee to register a domain, ranging from \$9 to several hundred dollars, depending on the top-level domain, such as .com. For more information, see [Route 53 Pricing for Domain Registration](#). This fee is not refundable.
- When you register a domain, we automatically create a hosted zone that has the same name as the domain. You use the hosted zone to specify where you want Route 53 to route traffic for your domain.
- During this tutorial, you create an Amazon S3 bucket and upload a sample web page. If you're a new AWS customer, you can get started with Amazon S3 for free. If you're an existing AWS customer, charges are based on how much data you store, on the number of requests for your data, and on the amount of data transferred. For more information, see [Amazon S3 Pricing](#).
- CloudFront charges are based on the number of requests for your data, the number of edge locations you use, and on the amount of data transferred. For more information, see [CloudFront Pricing](#).

Topics

- [Use your domain for a static website in an Amazon S3 bucket \(p. 17\)](#)
- [Use an Amazon CloudFront distribution to serve a static website \(p. 26\)](#)

Use your domain for a static website in an Amazon S3 bucket

This getting started tutorial shows you how to perform the following tasks:

- Register a domain name, such as example.com
- Create an Amazon S3 bucket and configure it to host a website
- Create a sample website and save the file in your S3 bucket
- Configure Amazon Route 53 to route traffic to your new website

When you're finished, you'll be able to open a browser, enter the name of your domain, and view your website.

Note

You can also transfer an existing domain to Route 53, but the process is more complex and time-consuming than registering a new domain. For more information, see [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#).

Topics

- [Prerequisites \(p. 18\)](#)
- [Step 1: Register a domain \(p. 18\)](#)
- [Step 2: Create an S3 bucket for your root domain \(p. 20\)](#)
- [Step 3 \(optional\): Create another S3 Bucket, for your subdomain \(p. 20\)](#)
- [Step 4: Set up your root domain bucket for website hosting \(p. 20\)](#)
- [Step 5 : \(optional\): Set up your subdomain bucket for website redirect \(p. 21\)](#)
- [Step 6: Upload index to create website content \(p. 22\)](#)
- [Step 7: Edit S3 Block Public Access settings \(p. 22\)](#)
- [Step 8: Attach a bucket policy \(p. 23\)](#)
- [Step 9: Test your domain endpoint \(p. 23\)](#)
- [Step 10: Route DNS traffic for your domain to your website bucket \(p. 24\)](#)
- [Step 11: Test your website \(p. 25\)](#)
- [Step 12 \(optional\): Use Amazon CloudFront to speed up distribution of your content \(p. 25\)](#)

Prerequisites

Before you begin, be sure that you've completed the steps in [Setting up Amazon Route 53 \(p. 13\)](#).

Step 1: Register a domain

To use a domain name (such as example.com), you must find a domain name that isn't already in use and register it. When you register a domain name, you reserve it for your exclusive use everywhere on the internet, typically for one year. By default, we automatically renew your domain name at the end of each year, but you can turn off automatic renewal.

To register a new domain using Amazon Route 53

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started**.
If you're already using Route 53, in the navigation pane, choose **Registered domains**.
3. Choose **Register Domain**.
4. Enter the domain name that you want to register, and choose **Check** to find out whether the domain name is available.
For information about how to specify characters other than a-z, 0-9, and - (hyphen), and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).
5. If the domain is available, choose **Add to cart**. The domain name appears in your shopping cart.

The **Related domain suggestions** list shows other domains that you might want to register instead of your first choice (if it's not available), or in addition to your first choice. Choose **Add to cart** for each additional domain that you want to register, up to a maximum of five domains.

If the domain name isn't available and you don't want one of the suggested domain names, repeat step 4 until you find an available domain name that you like.

Note

If you also want your users to be able to use `www.your-domain-name`, such as `www.example.com`, to access your sample website, you don't need to register a second domain. Later in this topic, we explain how to route traffic for `www.your-domain-name` to your website.

6. In the shopping cart, choose the number of years that you want to register the domain for.
7. To register more domains, repeat steps 4 through 6.
8. Choose **Continue**.
9. On the **Contact Details for Your n Domains** page, enter contact information for the domain registrant, administrator, and technical contacts.

By default, we use the same information for all three contacts. If you want to enter different information for one or more contacts, change the value of **My Registrant, Administrative, and Technical Contacts are all the same to No.**

If you're registering more than one domain, we use the same contact information for all of the domains.

For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

10. For some top-level domains (TLDs), we're required to collect additional information. For these TLDs, enter the applicable values after the **Postal/Zip Code** field.
11. Choose whether you want to hide your contact information from WHOIS queries. For more information, see the following topics:
 - [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#)
 - [Domains that you can register with Amazon Route 53 \(p. 97\)](#)
12. Choose **Continue**.
13. Review the information that you entered, read the terms of service, and select the check box to confirm that you've read the terms of service.
14. Choose **Complete Purchase**.

We send an email to the registrant for the domain to verify that the registrant contact can be reached at the email address that you specified. (This is an ICANN requirement.) The email comes from one of the following email addresses:

- noreply@registrar.amazon.com – for TLDs registered by Amazon Registrar.
- noreply@domainnameverification.net – for TLDs registered by our registrar associate, Gandi. To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Important

The registrant contact must follow the instructions in the email to confirm that the email was received, or we must suspend the domain as required by ICANN. When a domain is suspended, it's not accessible on the internet.

You'll receive another email when your domain registration has been approved. To determine the current status of your request, see [Viewing the status of a domain registration \(p. 52\)](#).

By default, you register a domain for one year. If you won't want to keep the domain, you can turn off automatic renewal, so the domain expires at the end of a year.

(Optional) To turn off automatic renewal for a domain

1. In the navigation pane, choose **Registered domains**.
2. In the list of domains, select the linked name of your domain.
3. If the value of the **Auto renew** field is **Enabled (disable)**, choose **disable** to turn off automatic renewal. The change takes effect immediately.

If the value of the field is **Disabled (enable)**, don't change the setting.

Step 2: Create an S3 bucket for your root domain

Amazon S3 lets you store and retrieve your data from anywhere on the internet. To organize your data, you create buckets and upload your data to the buckets by using the AWS Management Console. You can use Amazon S3 to host a static website in a bucket. The following procedure explains how to create a bucket.

To create an S3 bucket for your root domain

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Create bucket**.
3. Enter the following values:

Bucket name

Enter the name of your domain, such as **example.com**.

Region

Choose the Region closest to most of your users.

Make note of the Region that you choose; you'll need this information later in the process.

4. To accept the default settings and create the bucket, choose **Create bucket**.

Step 3 (optional): Create another S3 Bucket, for your subdomain

In the preceding procedure, you created a bucket for your domain name, such as example.com. This allows your users to access your website by using your domain name, such as example.com.

If you also want your users to be able to use **www.your-domain-name**, such as www.example.com, to access your sample website, create a second S3 bucket. Configure the second bucket to route traffic to the first bucket.

To create an S3 bucket for **www.your-domain-name**

1. Choose **Create bucket**.
2. Enter the following values:

Bucket name

Enter **www.your-domain-name**. For example, if you registered the domain name example.com, enter **www.example.com**.

Region

Choose the same Region that you created the first bucket in.

3. To accept the default settings and create the bucket, choose **Create**.

Step 4: Set up your root domain bucket for website hosting

Now that you have an S3 bucket, you can configure it for website hosting.

To allow website hosting on your S3 bucket

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to enable for static website hosting.
3. Choose **Properties**.
4. Under **Static website hosting**, choose **Enable**.
5. Choose **Use this bucket to host a website**.
6. Under **Static website hosting**, choose **Enable**.
7. In **Index document**, enter the file name of the index document, typically `index.html`.

The index document name is case sensitive and must exactly match the file name of the HTML index document that you plan to upload to your S3 bucket. When you configure a bucket for website hosting, you must specify an index document. Amazon S3 returns this index document when requests are made to the root domain or any of the subfolders.

8. (Optional) To provide your own custom error document for 4XX class errors, in **Error document**, enter the custom error document file name.

If you don't specify a custom error document and an error occurs, Amazon S3 returns a default HTML error document.

9. (Optional) If you want to specify advanced redirection rules, in **Redirection rules**, enter XML to describe the rules.

For more information, see [Configuring advanced conditional redirects](#) in the *Amazon Simple Storage Service User Guide*.

10. Choose **Save changes**.
11. Under **Static website hosting**, note the **Endpoint**.

The **Endpoint** is the Amazon S3 website endpoint for your bucket. After you finish configuring your bucket as a static website, you can use this endpoint to test your website, as shown in [Step 9: Test your domain endpoint \(p. 23\)](#).

After you use the following steps to edit settings for public access and add a bucket policy that allows public read access, you can use the website endpoint to access your website.

Step 5 : (optional): Set up your subdomain bucket for website redirect

After you configure your root domain bucket for website hosting, you can optionally configure your subdomain bucket to redirect all requests to the domain. For example, you can configure all requests for `www.example.com` to be redirected to `example.com`.

To configure a redirect

1. On the Amazon S3 console, in the **Buckets** list, choose your subdomain bucket name (for example, `www.example.com`).
2. Choose **Properties**.
3. Under **Static website hosting**, choose **Edit**.
4. Choose **Redirect requests for an object**.
5. In the **Target bucket** box, enter your root domain, for example, `example.com`.
6. For **Protocol**, choose `http`.

7. Choose **Save changes**.

Step 6: Upload index to create website content

When you allow static website hosting on your bucket, you enter the name of the index document (for example, `index.html`). After you allow static website hosting for the bucket, you upload an HTML file with this index document name to your bucket.

To upload an index file

1. Copy the following example text you can use as a simple one-page website for this tutorial, paste it into a text editor, and save it as `index.html`:

```
<html>
<head>
<title>Amazon Route 53 Getting Started</title>
</head>

<body>

<h1>Routing Internet Traffic to an Amazon S3 Bucket for Your Website</h1>

<p>For more information, see
<a href="https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-started.html">Getting Started with Amazon Route 53</a>
in the <emphasize>Amazon Route 53 Developer Guide</emphasize>.</p>

</body>

</html>
```

2. In the **Buckets list**, choose the name of the bucket that you want to enable static website hosting for.
3. In the Amazon S3 console, choose the name of the bucket that you created in the procedure [To allow website hosting on your S3 bucket \(p. 21\)](#) (click the linked bucket name).
4. Choose **Upload, Add Files**, select `index.html` from where you saved it, and then **Upload**.
5. If you created an error document, for example, `404.html`, follow steps 3 through 5 to upload it.

Step 7: Edit S3 Block Public Access settings

By default, Amazon S3 blocks public access to your account and buckets. If you want to use a bucket to host a static website, use these steps to edit your public access settings.

Warning

Before you complete this step, review [Blocking public access to your Amazon S3 storage](#) to ensure that you understand and accept the risks involved with allowing public access. When you turn off block public access settings to make your bucket public, anyone on the internet can access your bucket. We recommend that you block all public access to your buckets.

To route traffic to your website

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose the name of the bucket that you have configured as a static website.
3. Choose **Permissions**.
4. Under **Block public access (bucket settings)**, choose **Edit**.

5. Clear **Block all public access**, and choose **Save changes**.

Amazon S3 turns off Block Public Access settings for your bucket. To create a public, static website, you might also have to edit the [Block Public Access settings](#) for your account before adding a bucket policy. If account settings for Block Public Access are currently turned on, you see a note under **Block public access (bucket settings)**.

Step 8: Attach a bucket policy

After you edit Amazon S3 Block Public Access settings, you can add a bucket policy to grant public read access to your bucket. When you grant public read access, anyone on the internet can access your bucket.

Warning

Before you complete this step, review [Blocking public access to your Amazon S3 storage](#) to ensure that you understand and accept the risks involved with allowing public access. When you turn off block public access settings to make your bucket public, anyone on the internet can access your bucket. We recommend that you block all public access to your buckets.

To route traffic to your website

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Under **Buckets**, choose the name of your bucket.
3. Choose **Permissions**.
4. Under **Bucket Policy**, choose **Edit**.
5. Copy the following bucket policy and paste it into a text editor. This policy grants everyone on the internet ("Principal": "*") permission to get the files ("Action": ["s3:GetObject"]) in the S3 bucket that is associated with your domain name ("arn:aws:s3:::*your-domain-name*/*").

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Sid": "AddPerm",  
        "Effect": "Allow",  
        "Principal": "*",  
        "Action": [  
            "s3:GetObject"  
        ],  
        "Resource": [  
            "arn:aws:s3:::your-domain-name/*"  
        ]  
    }]  
}
```

6. Update the value for Resource to *your-domain-name*, for example **example.com**.
7. Choose **Save changes**.

Step 9: Test your domain endpoint

After you configure your domain bucket to host a public website, you can test your endpoint. You can test the endpoint only for your domain bucket because your subdomain bucket is set up for website redirect and not static website hosting.

Note

Amazon S3 does not support HTTPS access to the website. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3.

For more information, see [Requiring HTTPS for Communication Between Viewers and CloudFront](#).

1. Under **Buckets**, choose the name of your bucket.
2. Choose **Properties**.
3. At the bottom of the page, under **Static website hosting**, choose your **Bucket website endpoint**.

Your index document opens in a separate browser window.

Step 10: Route DNS traffic for your domain to your website bucket

You now have a one-page website in your S3 bucket. To start routing internet traffic for your domain to your S3 bucket, perform the following procedure.

To route traffic to your website

1. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.

Note

When you registered your domain, Amazon Route 53 automatically created a hosted zone with the same name. A hosted zone contains information about how you want Route 53 to route traffic for the domain.

3. In the list of hosted zones, choose the name of your domain.
4. Choose **Create record**.

Note

Each record contains information about how you want to route traffic for one domain (such as example.com) or one subdomain (such as www.example.com or test.example.com). Records are stored in the hosted zone for your domain.

5. Choose **Switch to wizard**.
6. Choose **Simple routing** and choose **Next**.
7. Choose **Define simple record**.
8. In **Record name**, accept the default value, which is the name of your hosted zone and your domain.
9. In **Record type**, choose **A - Routes traffic to an IPv4 address and some AWS resources**.
10. In **Value/Route traffic to**, choose **Alias to S3 website endpoint**.
11. Choose the Region.
12. Choose the S3 bucket.

The bucket name should match the name that appears in the **Name** box. In the **Choose S3 bucket** list, the bucket name appears with the Amazon S3 website endpoint for the Region where the bucket was created, for example, s3-website-us-west-1.amazonaws.com (example.com).

Choose S3 bucket lists a bucket if one of the following is true:

- You configured the bucket as a static website.
- The bucket name is the same as the name of the record that you're creating.
- The current AWS account created the bucket.

If your bucket does not appear in the **Choose S3 bucket** list, enter the Amazon S3 website endpoint for the Region where the bucket was created, for example, s3-website-us-

`west-2.amazonaws.com`. For a complete list of Amazon S3 website endpoints, see [Amazon S3 Website endpoints](#). For more information about the alias target, see "values/route traffic to" section in [Values specific for simple alias records \(p. 404\)](#).

13. For **Evaluate target health**, choose **No**.

14. Choose **Define simple record**.

(Optional) To add an alias record for your subdomain (`www.example.com`)

If you created a bucket for your subdomain, add an alias record for it also.

1. Under **Configure records**, choose **Define simple record**.
2. In **Record name** for your subdomain, type `www`.
3. In **Record type**, choose **A - Routes traffic to an IPv4 address and some AWS resources**.
4. In **Value/Route traffic to**, choose **Alias to S3 website endpoint**.
5. Choose the Region.
6. Choose the S3 bucket, for example, `s3-website-us-west-2.amazonaws.com` (`example.com`).

If your bucket does not appear in the **Choose S3 bucket** list, enter the Amazon S3 website endpoint for the Region where the bucket was created, for example, `s3-website-us-west-2.amazonaws.com`.

7. For **Evaluate target health**, choose **No**.
8. Choose **Define simple record**.
9. On the **Configure records** page, choose **Create records**.

Step 11: Test your website

To verify that the website is working correctly, open a web browser and browse to the following URLs:

- `http://your-domain-name`, for example, `example.com` – Displays the index document in the `your-domain-name` bucket
- `http://www.your-domain-name` for example, `www.example.com` – Redirects your request to the `your-domain-name` bucket

In some cases, you might need to clear the cache to see the expected behavior.

For more advanced information about routing your internet traffic, see [Configuring Amazon Route 53 as your DNS service \(p. 325\)](#). For information about routing your internet traffic to AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Step 12 (optional): Use Amazon CloudFront to speed up distribution of your content

CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

- If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

- If the content is not in that edge location, CloudFront retrieves it from an Amazon S3 bucket or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

For information about using CloudFront to distribute the content in your Amazon S3 bucket, see [Adding CloudFront when you're distributing content from Amazon S3](#) in the *Amazon CloudFront Developer Guide*.

Use an Amazon CloudFront distribution to serve a static website

This getting started tutorial shows you how to perform the following tasks:

- Register a domain name, such as example.com.
- Create a certificate for your domain.
- Create two Amazon S3 buckets and configure one to host a website and the other one to redirect to the subdomain.
- Create a sample website and save the file in your S3 bucket.
- Create CloudFront distributions for both S3 buckets.
- Configure Amazon Route 53 to route traffic to the CloudFront distributions.

When you're finished, you'll be able to open a browser, enter the name of your domain, and view your website securely.

Topics

- [Prerequisites \(p. 26\)](#)
- [Step 1: Register a domain \(p. 26\)](#)
- [Step 2: Request a public certificate \(p. 28\)](#)
- [Step 3: Create an S3 bucket to host your subdomain \(p. 29\)](#)
- [Step 4 : Create another S3 bucket, for your root domain \(p. 29\)](#)
- [Step 5: Upload website files to your subdomain bucket \(p. 30\)](#)
- [Step 6: Set up your root domain bucket for website redirect \(p. 30\)](#)
- [Step 7: Create an Amazon CloudFront distribution for your subdomain \(p. 31\)](#)
- [Step 8: Create an Amazon CloudFront distribution for your root domain \(p. 31\)](#)
- [Step 9: Route DNS traffic for your domain to your CloudFront distribution \(p. 32\)](#)
- [Step 10 : Test your website \(p. 33\)](#)

Prerequisites

Before you begin, be sure that you've completed the steps in [Setting up Amazon Route 53 \(p. 13\)](#).

Step 1: Register a domain

To use a domain name (such as example.com), you must find a domain name that isn't already in use and register it. When you register a domain name, you reserve it for your exclusive use everywhere on the

internet, typically for one year. By default, we automatically renew your domain name at the end of each year, but you can turn off automatic renewal.

To register a new domain using Amazon Route 53

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started**.
If you're already using Route 53, in the navigation pane, choose **Registered domains**.
3. Choose **Register Domain**.
4. Enter the domain name that you want to register, and choose **Check** to find out whether the domain name is available.
For information about how to specify characters other than a-z, 0-9, and - (hyphen), and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).
5. If the domain is available, choose **Add to cart**. The domain name appears in your shopping cart.

The **Related domain suggestions** list shows other domains that you might want to register instead of your first choice (if it's not available), or in addition to your first choice. Choose **Add to cart** for each additional domain that you want to register, up to a maximum of five domains.

If the domain name isn't available and you don't want one of the suggested domain names, repeat step 4 until you find an available domain name that you like.

Note

If you also want your users to be able to use `www.your-domain-name`, such as `www.example.com`, to access your sample website, you don't need to register a second domain. Later in this topic, we explain how to route traffic for `www.your-domain-name` to your website.

6. In the shopping cart, choose the number of years that you want to register the domain for.
7. To register more domains, repeat steps 4 through 6.
8. Choose **Continue**.
9. On the **Contact Details for Your n Domains** page, enter contact information for the domain registrant, administrator, and technical contacts.

By default, we use the same information for all three contacts. If you want to enter different information for one or more contacts, change the value of **My Registrant, Administrative, and Technical Contacts are all the same** to **No**.

If you're registering more than one domain, we use the same contact information for all of the domains.

For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

10. For some top-level domains (TLDs), we're required to collect additional information. For these TLDs, enter the applicable values after the **Postal/Zip Code** field.
11. Choose whether you want to hide your contact information from WHOIS queries. For more information, see the following topics:
 - [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#)
 - [Domains that you can register with Amazon Route 53 \(p. 97\)](#)
12. Choose **Continue**.
13. Review the information that you entered, read the terms of service, and select the check box to confirm that you've read the terms of service.
14. Choose **Complete Purchase**.

We send an email to the registrant for the domain to verify that the registrant contact can be reached at the email address that you specified. (This is an ICANN requirement.) The email comes from one of the following email addresses:

- noreply@registrar.amazon.com – for TLDs registered by Amazon Registrar.
- noreply@domainnameverification.net – for TLDs registered by our registrar associate, Gandi. To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Important

The registrant contact must follow the instructions in the email to confirm that the email was received, or we must suspend the domain as required by ICANN. When a domain is suspended, it's not accessible on the internet.

You'll receive another email when your domain registration has been approved. To determine the current status of your request, see [Viewing the status of a domain registration \(p. 52\)](#).

By default, you register a domain for one year. If you won't want to keep the domain, you can deactivate automatic renewal, so the domain expires at the end of a year.

(Optional) To turn off automatic renewal for a domain

1. In the navigation pane, choose **Registered domains**.
2. In the list of domains, select the linked name of your domain.
3. If the value of the **Auto renew** field is **Enabled (disable)**, choose **disable** to turn off automatic renewal. The change takes effect immediately.

If the value of the field is **Disabled (enable)**, don't change the setting.

Step 2: Request a public certificate

A public certificate is required for your Amazon CloudFront distributions to configure CloudFront to require that viewers use HTTPS so that connections are encrypted when CloudFront communicates with viewers.

To request an AWS Certificate Manager(ACM) public certificate (console)

1. Sign in to the AWS Management Console and open the ACM console at <https://console.aws.amazon.com/acm/home>.

Note

Make sure you create the certificate in the US East (N. Virginia) Region. This is required for Amazon CloudFront.

Choose **Request a public certificate** and then **Request a certificate**.

2. Under **Domain name**, enter your domain, such as `example.com`.

Under **Add another name to this certificate**, enter an asterisk in front of the domain name to request a wildcard certificate for all subdomains, such as `*.example.com`.

3. Choose **Next**.
4. On the **Select validation method** page, choose **DNS validation** and then **Next**.
5. On the **Add tags** page, you can optionally tag your certificate. Tags are key-value pairs that serve as metadata for identifying and organizing AWS resources.

When you finish adding tags, choose **Review**.

6. On the **Review** page, make sure the information you entered is correct, and then choose **Confirm and request**.
7. On the **Validation** page, expand both domains and choose **Create record in Route 53** to automatically add the CNAME records for your domains, and then choose **Create**.

After **Success** is displayed for both domains, choose **Continue** on the bottom of the page.

Step 3: Create an S3 bucket to host your subdomain

To create an S3 bucket for *www.your-domain-name*

Amazon S3 lets you store and retrieve your data from anywhere on the internet. In this step you create an S3 bucket to store all the files for your website.

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Create bucket**.
3. Enter the following values:

Bucket name

Enter **www.your-domain-name**. For example, if you registered the domain name example.com, enter **www.example.com**.

Region

Choose a Region for your bucket.

4. To accept the default settings and create the bucket, choose **Create bucket**.

For more information about the S3 bucket settings, see [View bucket properties](#) in the *Amazon S3 user guide*.

Step 4 : Create another S3 bucket, for your root domain

If you also want your users to be able to use the root domain, *your-domain-name* (such as example.com) to access your sample website, create a second S3 bucket. You then configure the second bucket to route traffic to the first bucket.

To create an S3 bucket for *your-domain-name*

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Create bucket**.
3. Enter the following values:

Bucket name

Enter **your-domain-name**. For example, if you registered the domain name example.com, enter **example.com**.

Region

Choose the same Region that you created the first bucket in.

4. To accept the default settings and create the bucket, choose **Create bucket**.

Step 5: Upload website files to your subdomain bucket

Now that you have an S3 bucket, you can upload your website files. In this tutorial you will just upload a simple index.html file that displays text on a page..

To enable your S3 bucket for website hosting

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the linked name of the bucket you want to upload the website files to, such as **www.example.com**.
3. Copy the example text that creates a simple one-page website, paste it into a text editor, and save it as index.html:

```
<html>
<head>
<title>Amazon Route 53 Getting Started</title>
</head>

<body>

<h1>Routing Internet traffic to Cloudfront distributions for your website stored in an
S3 bucket</h1>

<p>For more information, see
<a href="https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-
started.html">Getting Started with Amazon Route 53</a>
in the <emphasize>Amazon Route 53 Developer Guide</emphasize>.</p>

</body>

</html>
```

4. In the **Objects** tab choose **Upload**.
5. Under **Files and folders**, choose **Add files** and upload your website files. For this tutorial, upload the index.html file you saved in step 3.

Step 6: Set up your root domain bucket for website redirect

After you configure your root domain bucket for website hosting, you can optionally configure your subdomain bucket to redirect all requests to the domain. For example, you can configure all requests for **example.com** to be redirected to **www.example.com**.

To configure a redirect

1. On the Amazon S3 console, in the **Buckets** list, choose your bucket name (for example, **example.com**).
2. Choose **Properties**.
3. Under **Static website hosting**, choose **Edit**.
4. Under **Static website hosting**, select **Enable**.
5. Choose **Redirect requests for an object**.
6. In the **Host name** box, enter your subdomain, for example, **www.example.com**.
7. For **Protocol**, choose **https**.

8. Choose **Save changes**.
9. Under **Static website hosting**, note the **Endpoint**.

The **Endpoint** is the Amazon S3 website endpoint for your bucket. You will use this endpoint to set up an Amazon CloudFront distribution.

Step 7: Create an Amazon CloudFront distribution for your subdomain

In this step you create a CloudFront distribution for your subdomain, such as `www.example.com`, to enable your website to use HTTPS so people can view it securely.

To create a CloudFront distribution

1. Open the CloudFront console at <https://console.aws.amazon.com/cloudfront/v3/home>.
2. Choose **Create Distribution**.
3. Under **Origin Settings**, for **Origin Domain Name**, choose the Amazon S3 bucket that you [created previously](#) (p. 29).

For **S3 bucket access**, select **Yes, use OAI (bucket can restrict access to only CloudFront)**. For the **Origin access identity**, you can choose from the list, or choose **Create new OAI** (both will work).

For **Bucket policy**, select **Yes, update the bucket policy**.

4. For the settings under **Default Cache Behavior Settings**, under **Viewer**, set **Viewer protocol policy** to **Redirect HTTP to HTTPS** and accept the default values for the rest.

For more information about cache behavior options, see [Cache behavior settings](#) in the *Amazon CloudFront developer guide*.

5. For the fields under **Settings**, do the following:

- Choose **Add item** for **Alternate domain name (CNAME) - optional**, and enter your subdomain, such as `www.example.com`.
- For **Custom SSL Certificate**, choose the certificate you [created previously](#) (p. 28).
- In the **Default root object** text box, type in `index.html`.
- For the rest, accept the default values.

For more information about distribution options, see [Distribution settings](#).

6. At the bottom of the page, choose **Create Distribution**.
7. After CloudFront creates your distribution, the value of the **Status** column for your distribution changes from **In Progress** to **Deployed**. This typically takes a few minutes.

Record the domain name that CloudFront assigns to your distribution, which appears in the list of distributions. You can use this domain name to test the distribution.

Step 8: Create an Amazon CloudFront distribution for your root domain

In this step you create a CloudFront distribution for your root domain to have it use HTTPS when its URL is redirected to the subdomain.

To create a CloudFront distribution

1. Open the CloudFront console at <https://console.aws.amazon.com/cloudfront/v3/home>.
2. Choose **Create Distribution**.
3. Under **Origin Settings**, for **Origin Domain Name**, enter the bucket website endpoint. You get this from the **Static website hosting** section of **Properties** for the Amazon S3 bucket that you [created previously \(p. 29\)](#).

For the rest, accept the default values.

4. For the fields under **Default Cache Behavior Settings**, do the following:
 - Under **Viewer**, set **Viewer protocol policy** to **Redirect HTTP to HTTPS**.
 - Set **Cache settings** to **CachingDisabled**.
 - Accept the default values for the rest.

For more information about cache behavior options, see [Cache behavior settings](#) in the *Amazon CloudFront developer guide*.

5. For the fields under **Settings**, do the following:
 - Choose **Add item** for **Alternate domain name (CNAME) - optional**, and enter your root domain, such as **example.com**.
 - For **Custom SSL Certificate**, choose the certificate you [created previously \(p. 28\)](#).
 - For the rest, accept the default values.

For more information about distribution options, see [Distribution settings](#).

6. At the bottom of the page, choose **Create Distribution**.
7. After CloudFront creates your distribution, the value of the **Status** column for your distribution changes from **In Progress** to **Deployed**. This typically takes a few minutes.

Record the domain name that CloudFront assigns to your distribution, which appears in the list of distributions. You can use this domain name to test the distribution,

Step 9: Route DNS traffic for your domain to your CloudFront distribution

You now have a one-page website in your S3 bucket that uses a CloudFront distribution. To start routing internet traffic for your domain to the CloudFront distribution, perform the following procedure.

For more information about routing traffic to CloudFront distributions, see [Routing traffic to an Amazon CloudFront distribution by using your domain name \(p. 498\)](#).

To route traffic to your website

1. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.

Note

When you registered your domain, Amazon Route 53 automatically created a hosted zone with the same name. A hosted zone contains information about how you want Route 53 to route traffic for the domain.

3. In the list of hosted zones, choose the name of your domain.
4. Choose **Create record**.

If you are in the **Quick create record** view, choose **Switch to wizard**.

Note

Each record contains information about how you want to route traffic for one domain (such as example.com) or subdomain (such as www.example.com or test.example.com). Records are stored in the hosted zone for your domain.

5. Choose **Simple routing** and choose **Next**.
6. Choose **Define simple record**.
7. In **Record name**, type in **www** in front of the default value, which is the name of your hosted zone and your domain.
8. In **Record type**, choose **A - Routes traffic to an IPv4 address and some AWS resources**.
9. In **Value/Route traffic to**, choose **Alias to CloudFront distribution**.
10. Choose the distribution.

The distribution name should match the name that appears in the **Domain name** box in the **Distributions** list, for example, dddjjjkkk.cloudfront.net.

11. For **Evaluate target health**, choose **No**.
12. Choose **Define simple record**.

To add an alias record for your root domain (example.com)

Add an alias record for your root domain also, so it points to the S3 bucket that redirects traffic to www.example.com. For more information about routing traffic to CloudFront distributions, see [Routing traffic to an Amazon CloudFront distribution by using your domain name \(p. 498\)](#).

1. Under **Configure records**, choose **Define simple record**.
2. In **Record name**, accept the default value.
3. In **Record type**, choose **A - Routes traffic to an IPv4 address and some AWS resources**.
4. In **Value/Route traffic to**, choose **Alias to CloudFront distribution**.
5. Choose the distribution.

The distribution name should match the name that appears in the **Domain name** box in the **Distributions** list, for example, dddjjjkkk.cloudfront.net.

6. For **Evaluate target health**, choose **No**.
7. Choose **Define simple record**.
8. On the **Configure records** page, choose **Create records**.

Step 10 : Test your website

To verify that the website is working correctly, open a web browser and browse to the following URLs:

- <https://www.your-domain-name>, for example, www.example.com – Displays the index document in the **www.your-domain-name** bucket
- <https://your-domain-name> for example, example.com – Redirects your request to the **www.your-domain-name** bucket

In some cases, you might need to clear the cache to see the expected behavior.

For more advanced information about routing your internet traffic, see [Configuring Amazon Route 53 as your DNS service \(p. 325\)](#). For information about routing your internet traffic to AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Integration with other services

You can integrate Amazon Route 53 with other AWS services to log requests that are sent to the Route 53 API, monitor the status of your resources, and assign tags to your resources. In addition, you can use Route 53 to route internet traffic to your AWS resources.

Topics

- [Logging, monitoring, and tagging \(p. 35\)](#)
- [Routing traffic to other AWS resources \(p. 35\)](#)

Logging, monitoring, and tagging

AWS CloudTrail

Amazon Route 53 is integrated with AWS CloudTrail, a service that captures information about every request that is sent to the Route 53 API by your AWS account. You can use information in the CloudTrail log files to determine which requests were made to Route 53, the source IP address from which each request was made, who made the request, when it was made, and so on.

For more information, see [Logging Amazon Route 53 API calls with AWS CloudTrail \(p. 635\)](#).

Amazon CloudWatch

You can use Amazon CloudWatch to monitor the status—healthy or unhealthy—of your Route 53 health checks. Health checks monitor the health and performance of your web applications, web servers, and other resources. At regular intervals that you specify, Route 53 submits automated requests over the internet to your application, server, or other resource to verify that it's reachable, available, and functional.

For more information, see [Monitoring health checks using CloudWatch \(p. 532\)](#).

Tag Editor

A tag is a label that you assign to an AWS resource, including Route 53 domains, hosted zones, and health checks. Each tag consists of a key and a value, both of which you define. For example, you might assign a tag to a domain registration that has the key "Customer" and the value "Example Corp." You can use tags for a variety of purposes; one common use is to categorize and track your AWS costs.

For more information, see [Tagging Amazon Route 53 resources \(p. 655\)](#).

Routing traffic to other AWS resources

You can use Amazon Route 53 to route traffic to a variety of AWS resources.

Amazon API Gateway

Amazon API Gateway lets you create, publish, maintain, monitor, and secure APIs at any scale. You can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud.

You can use Route 53 to route traffic to an API Gateway API. For more information, see [Routing traffic to an Amazon API Gateway API by using your domain name \(p. 496\)](#).

Amazon CloudFront

To speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website—including dynamic, static, streaming, and interactive content—by using a global network of edge locations. CloudFront routes requests for your content to the edge location that gives your users the lowest latency. You can use Route 53 to route traffic for your domain to your CloudFront distribution. For more information, see [Routing traffic to an Amazon CloudFront distribution by using your domain name \(p. 498\)](#).

Amazon EC2

Amazon EC2 provides scalable computing capacity in the AWS Cloud. You can launch an EC2 virtual computing environment (an instance) using a preconfigured template (an Amazon Machine Image, or AMI). When you launch an EC2 instance, EC2 automatically installs the operating system (Linux or Microsoft Windows) and additional software included in the AMI, such as web server or database software.

If you host a website or run a web application on an EC2 instance, you can route traffic for your domain, such as example.com, to your server by using Route 53. For more information, see [Routing traffic to an Amazon EC2 instance \(p. 500\)](#).

AWS Elastic Beanstalk

If you use AWS Elastic Beanstalk to deploy and manage applications in the AWS Cloud, you can use Route 53 to route DNS traffic for your domain, such as example.com, to an Elastic Beanstalk environment. For more information, see [Routing traffic to an AWS Elastic Beanstalk environment \(p. 502\)](#).

Elastic Load Balancing

If you host a website on multiple Amazon EC2 instances, you can distribute traffic to your website across the instances by using an Elastic Load Balancing (ELB) load balancer. The ELB service automatically scales the load balancer as traffic to your website changes over time. The load balancer also can monitor the health of its registered instances and route domain traffic only to healthy instances.

You can use Route 53 to route traffic for your domain to your Classic, Application, or Network Load Balancer. For more information, see [Routing traffic to an ELB load balancer \(p. 505\)](#).

Amazon Lightsail

Amazon Lightsail provides compute, storage, and networking capacity and capabilities to deploy and manage websites, web applications, and databases in the cloud for a low, predictable monthly price.

If you use Lightsail, you can use Route 53 to route traffic to your Lightsail instance. For more information, see [Using Route 53 to point a domain to an Amazon Lightsail instance](#).

Amazon S3

Amazon Simple Storage Service (Amazon S3) provides secure, durable, highly scalable cloud storage. You can configure an S3 bucket to host a static website that can include web pages and client-side scripts. (S3 doesn't support server-side scripting.) You can use Route 53 to route traffic to an Amazon S3 bucket. For more information, see the following topics:

- For information about routing traffic to a bucket, see [Routing traffic to a website that is hosted in an Amazon S3 bucket \(p. 507\)](#).
- For a more detailed explanation of how to host a static website in an S3 bucket, see [Getting started with Amazon Route 53 \(p. 17\)](#).

Amazon Virtual Private Cloud (Amazon VPC)

An interface endpoint lets you connect to services that are powered by AWS PrivateLink. These services include some AWS services, services hosted by other AWS customers and partners in their own VPCs (referred to as *endpoint services*), and supported AWS Marketplace partner services.

You can use Route 53 to route traffic to an interface endpoint. For more information, see [Routing traffic to an Amazon Virtual Private Cloud interface endpoint by using your domain name \(p. 509\)](#).

Amazon WorkMail

If you're using Amazon WorkMail for your business email and you're using Route 53 as your DNS service, you can use Route 53 to route traffic to your Amazon WorkMail email domain. For more information, see [Routing traffic to Amazon WorkMail \(p. 511\)](#).

For more information see [Routing internet traffic to your AWS resources \(p. 496\)](#).

DNS domain name format

Domain names (including the names of domains, hosted zones, and records) consist of a series of labels separated by dots. Each label can be up to 63 bytes long. The total length of a domain name cannot exceed 255 bytes, including the dots. Amazon Route 53 supports any valid domain name.

Naming requirements depend on whether you're registering a domain name or you're specifying the name of a hosted zone or a record. See the applicable topic.

Topics

- [Formatting domain names for domain name registration \(p. 38\)](#)
- [Formatting domain names for hosted zones and records \(p. 38\)](#)
- [Using an asterisk \(*\) in the names of hosted zones and records \(p. 39\)](#)
- [Formatting internationalized domain names \(p. 40\)](#)

Formatting domain names for domain name registration

For domain name registration, a domain name can contain only the characters a-z, 0-9, and - (hyphen). You can't specify a hyphen at the beginning or end of a label.

For information about how to register an internationalized domain name (IDN), see [Formatting internationalized domain names \(p. 40\)](#).

Formatting domain names for hosted zones and records

For hosted zones and records, the domain name can include any of the following printable ASCII characters (excluding spaces):

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

Amazon Route 53 stores alphabetic characters as lowercase letters (a-z), regardless of how you specify them: as uppercase letters, lowercase letters, or the corresponding letters in escape codes.

If your domain name contains any of the following characters, you must specify the characters by using escape codes in the format `\three-digit octal code`:

- Characters 000 to 040 octal (0 to 32 decimal, 0x00 to 0x20 hexadecimal)
- Characters 177 to 377 octal (127 to 255 decimal, 0x7F to 0xFF hexadecimal)
- . (period), character 056 octal (46 decimal, 0x2E hexadecimal), when used as a character in a domain name. When using . as a delimiter between labels, you do not need to use an escape code.

For example, to create a hosted zone for exämpel.com, you specify ex\344mple.com.

If the domain name includes any characters other than a to z, 0 to 9, - (hyphen), or _ (underscore), Route 53 API actions return the characters as escape codes. This is true whether you specify the characters as characters or as escape codes when you create the entity. The Route 53 console displays the characters as characters, not as escape codes.

For a list of ASCII characters the corresponding octal codes, do an internet search on "ascii table".

To specify an internationalized domain name (IDN), convert the name to Punycode. For more information, see [Formatting internationalized domain names \(p. 40\)](#).

Using an asterisk (*) in the names of hosted zones and records

You can create hosted zones and records that include * in the name.

Hosted zones

- You can't include an * in the leftmost label in a domain name. For example, *.example.com is not allowed.
- If you include * in other positions, DNS treats it as an * character (ASCII 42), not as a wildcard.

Records

DNS treats the * character either as a wildcard or as the * character (ASCII 42), depending on where it appears in the name. Note the following restrictions on using * as a wildcard in the name of a record:

- The * must replace the leftmost label in a domain name, for example, *.example.com or *.acme.example.com. If you include * in any other position, such as prod.*.example.com, DNS treats it as an * character (ASCII 42), not as a wildcard.
- The * must replace the entire label. For example, you can't specify *prod.example.com or prod*.example.com.
- Specific domain names take precedence. For example, if you create records for *.example.com and acme.example.com, Route 53 always responds to DNS queries for acme.example.com with the values in the acme.example.com record.
- The * applies to DNS queries for the subdomain level that includes the asterisk, and all the subdomains of that subdomain. For example, if you create a record named *.example.com, Route 53 uses the values in that record to respond to DNS queries for zenith.example.com, acme.zenith.example.com, and pinnacle.acme.zenith.example.com (if there are no records that have those names).

If you create a record named *.example.com and there's no example.com record, Route 53 responds to DNS queries for example.com with NXDOMAIN (non-existent domain).

- You can configure Route 53 to return the same response to DNS queries both for all subdomains at the same level and for the domain name. For example, you can configure Route 53 to respond to DNS queries such as acme.example.com and zenith.example.com using the example.com record. Perform the following steps:
 1. Create a record for the domain, such as example.com.
 2. Create an alias record for the subdomain, such as *.example.com. Specify the record that you created in step 1 as the target for the alias record.
- You can't use the * as a wildcard for records that have a type of NS.

Formatting internationalized domain names

When you register a new domain name or create hosted zones and records, you can specify letters other than a-z (for example, the ç in French), characters in other alphabets (for example, Cyrillic or Arabic), and characters in Chinese, Japanese, or Korean. Amazon Route 53 stores these internationalized domain names (IDNs) in Punycode, which represents Unicode characters as ASCII strings.

If you're registering a domain name, note the following:

- You can use characters other than a-z, 0-9, and - (hyphen) only if the top-level domain (TLD) supports IDNs and supports the language that you want to use. To determine which languages a TLD supports, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).
- You can specify a name in an unsupported language if the name contains only the letters a-z. For example, if a TLD doesn't support French but the name that you want to use includes only the characters a-z without diacritical marks, you can still use that name. In this example, a name that includes a "c" is allowed; a name that contains a "ç" is not.
- If a TLD doesn't support IDNs or doesn't support the language that you want to use for your domain name, you also can't specify the name in Punycode even though the Punycode includes only a-z, 0-9, and -.

The following example shows the Punycode representation of the internationalized domain name 中國.asia:

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

When you enter an IDN in the address bar of a modern browser, the browser converts it to Punycode before submitting a DNS query or making an HTTP request.

How you enter an IDN depends on what you're creating (domain names, hosted zones, or records), and how you're creating it (API, SDK, or Route 53 console):

- If you're using the Route 53 API or one of the AWS SDKs, you can programmatically convert a Unicode value to Punycode. For example, if you're using Java, you can convert a Unicode value to Punycode by using the `toASCII` method of the `java.net.IDN` library.
- If you're using the Route 53 console to register a domain name, you can paste the name, including Unicode characters, into the name field, and the console converts the value to Punycode before saving it.
- If you're using the Route 53 console to create hosted zones or records, you need to convert the domain name to Punycode before you enter the name in the applicable **Name** field. For information about online converters, perform an internet search on "punycode converter".

If you're registering a domain name, note that not all top-level domains (TLDs) support IDNs. For a list of TLDs supported by Route 53, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#). TLDs that don't support IDNs are noted.

Registering domain names using Amazon Route 53

When you want to get a new domain name, such as the **example.com** part of the URL `http://example.com`, you can register it with Amazon Route 53. You can also transfer the registration for existing domains from other registrars to Route 53 or transfer the registration for domains that you register with Route 53 to another registrar.

The procedures in this chapter explain how to register and transfer domains using the Route 53 console, and how to edit domain settings and view domain status. If you're only registering and managing a few domains, using the console is the easiest way.

If you need to register and manage a lot of domains, you might prefer to make changes programmatically. For more information, see [Setting up Amazon Route 53 \(p. 13\)](#).

Note

If you are using a language for which an AWS SDK exists, use the SDK rather than trying to work your way through the APIs. The SDKs make authentication simpler, integrate easily with your development environment, and provide easy access to Route 53 commands.

Domain name registration services are provided under our [Domain Name Registration Agreement](#).

Topics

- [Registering domains \(p. 41\)](#)
- [Updating settings for a domain \(p. 52\)](#)
- [Renewing registration for a domain \(p. 63\)](#)
- [Restoring an expired or deleted domain \(p. 65\)](#)
- [Replacing the hosted zone for a domain that is registered with Route 53 \(p. 66\)](#)
- [Transferring domains \(p. 67\)](#)
- [Resending authorization and confirmation emails \(p. 86\)](#)
- [Configuring DNSSEC for a domain \(p. 89\)](#)
- [Viewing information about domains that are registered with Amazon Registrar \(p. 93\)](#)
- [Deleting a domain name registration \(p. 93\)](#)
- [Contacting AWS Support about domain registration issues \(p. 95\)](#)
- [Downloading a domain billing report \(p. 96\)](#)
- [Domains that you can register with Amazon Route 53 \(p. 97\)](#)

Registering domains

For information about registering new domains, see the applicable topic.

Topics

- [Registering a new domain \(p. 42\)](#)
- [Values that you specify when you register or transfer a domain \(p. 47\)](#)
- [Values that Amazon Route 53 returns when you register a domain \(p. 51\)](#)
- [Viewing the status of a domain registration \(p. 52\)](#)

Registering a new domain

Register or add a new domain

You can use Amazon Route 53 with domains you register with Route 53, and with domains you have registered with other DNS providers. Depending on your DNS provider, choose one of the following procedures to register and use a new domain with Route 53:

- For registering a new domain, see [register a new domain \(p. 43\)](#).
- For an existing domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).
- For moving a domain to another registrar, see [update nameservers when you want to use another DNS service \(p. 46\)](#).

Considerations for domain registration

Before you start, note the following:

Contacting AWS Support

If you encounter issues while registering a domain, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Domain registration pricing

For information about the cost to register domains, see [Amazon Route 53 Pricing for Domain Registration](#).

Supported domains

For a list of supported TLDs, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

You can't change a domain name after you register it

If you accidentally register the wrong domain name, you can't change it. Instead, you need to register another domain name and specify the correct name. You also can't get a refund for a domain name that you registered accidentally.

AWS credits

You can't use AWS credits to pay the fee for registering a new domain with Route 53.

Special or premium prices

TLD registries have assigned special or premium prices to some domain names. You can't use Route 53 to register a domain that has a special or premium price.

Charges for hosted zones

When you register a domain with Route 53, we automatically create a hosted zone for the domain and charge a small monthly fee for the hosted zone in addition to the annual charge for the domain registration. This hosted zone is where you store information about how to route traffic for your

domain, for example, to an Amazon EC2 instance or a CloudFront distribution. If you don't want to use your domain right now, you can delete the hosted zone; if you delete it within 12 hours of registering the domain, there won't be any charge for the hosted zone on your AWS bill. We also charge a small fee for the DNS queries that we receive for your domain. For more information, see [Amazon Route 53 Pricing](#).

Replacing the hosted zone for a domain

If you create a new hosted zone for a domain, you must also update the nameservers for the domain to use the same nameservers as the new hosted zone. For details see, [Replacing the hosted zone for a domain that is registered with Route 53 \(p. 66\)](#)

To register a new domain using Route 53

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started**.
If you're already using Route 53, in the navigation pane, choose **Registered domains**.
3. Choose **Register domain**, and specify the domain that you want to register:
 - a. Enter the domain name that you want to register, and choose **Check** to find out whether the domain name is available.
If the domain name that you want to register contains characters other than a-z, A-Z, 0-9, and - (hyphen), note the following:
 - You can enter the name using the applicable characters. You don't need to convert the name to Punycode.
 - A list of languages appears. Choose the language of the specified name. For example, if you enter příklad ("example" in Czech), choose Czech (CES) or Czech (CZE).

Note

For languages that have more than one code, you might need to try both of them.
Even though CES and CZE are synonymous, some TLD registries support only one or the other.

- b. If the domain is available, choose **Add to cart**. The domain name appears in your shopping cart.
The **Related domain suggestions** list shows other domains that you might want to register instead of your first choice (if it's not available) or in addition to your first choice. Choose **Add to cart** for each additional domain that you want to register, up to a maximum of five domains.
 - c. In the shopping cart, choose the number of years that you want to register the domain for.
 - d. To register more domains, repeat steps 3a through 3c.
4. Choose **Continue**.
5. On the **Contact Details for Your n Domains** page, enter contact information for the domain registrant, administrator, and technical contacts. The values that you enter here are applied to all of the domains that you're registering. For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

Note the following considerations:

First Name and Last Name

For **First Name and Last Name**, we recommend that you specify the name on your official ID. For some changes to domain settings, some domain registries require that you provide proof of identity. The name on your ID must match the name of the registrant contact for the domain.

Different contacts

By default, we use the same information for all three contacts. If you want to enter different information for one or more contacts, change the value of **My Registrant, Administrative, and Technical Contacts are all the same to No.**

Note

For .it domains, the registrant and administrative contacts must be the same.

Multiple domains

If you're registering more than one domain, we use the same contact information for all of the domains.

Additional required information

For some top-level domains (TLDs), we're required to collect additional information. For these TLDs, enter the applicable values after the **Postal/Zip Code** field.

Privacy protection

Choose whether you want to hide your contact information from WHOIS queries.

Note

You must specify the same privacy setting for the administrative, registrant, and technical contacts.

For more information, see the following topics:

- [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#)
- [Domains that you can register with Amazon Route 53 \(p. 97\)](#)

Note

To enable privacy protection for .co.uk, .me.uk, and .org.uk domains, you must open a support case and request privacy protection.

6. Choose **Continue**.
7. **Some TLDs only** – If you specified an email address for the registrant contact that has never been used to register a domain with Route 53, some TLD registries require you to verify that the address is valid.

If the registry requires verification and if it's possible to verify the address during domain registration, the console displays a **Verify the Email Address for the Registrant Contact** section:

- If the section doesn't appear, skip to step 8.
- If the section appears and the status is **email-address is verified**, skip to step 8.
- If the section appears and the value is **Registrant email not verified**, continue with this step.

Perform the following steps:

- a. Choose **Send verification email**. We send a verification email from one of the following email addresses:
 - **noreply@registrar.amazon.com** – for TLDs registered by Amazon Registrar.
 - **noreply@domainnameverification.net** – for TLDs registered by our registrar associate, Gandi. To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Important

The registrant contact must follow the instructions in the email to verify that the email was received, or we must suspend the domain as required by ICANN. When a domain is suspended, it's not accessible on the internet.

- b. When you receive the verification email, choose the link in the email that verifies that the email address is valid. If you don't receive the email immediately, check your junk email folder.
- c. Return to the Route 53 console. If the status doesn't automatically update to say **email-address is verified**, choose **Refresh status**.
8. Choose whether you want us to automatically renew your domain registration before the expiration date.

Note

Domain name registrations and renewals are not refundable. If you enable automatic domain renewal and you decide that you don't want the domain name after we renew the registration, you can't get a refund for the cost of the renewal.

9. Review the information that you entered, read the terms of service, and select the check box to confirm that you've read the terms of service.
10. Choose **Complete Purchase**.
11. **AISPL (India) customers only:** If your contact address is in India, your user agreement is with Amazon Internet Services Pvt. Ltd (AISPL), a local AWS seller in India. To register a domain with Route 53, perform the following steps to pay the fee for registering your domain.
 - a. Go to the [Orders and Invoices](#) page in the AWS Management Console.
 - b. In the **Payments Due** section, find the applicable invoice.
 - c. In the **Actions** column, choose **Verify and Pay**.

After you pay the invoice, we complete the domain registration and send the applicable emails.

Important

If you don't pay the invoice within five days, the invoice is canceled. To register a domain after an invoice is canceled, resubmit the request.

For more information, see [Managing your payments in India](#) in the *AWS Billing and Cost Management User Guide*.

12. **Generic TLDs only** – Verify that the email address for the registrant contact is valid.

Note

If you were able to verify your email address in step 7, skip to step 13.

If the registry requires us to verify the email address for the registrant contact but doesn't allow us to verify earlier in the process, we send a verification email from one of the following email addresses:

- noreply@registrar.amazon.com – for TLDs registered by Amazon Registrar.
- noreply@domainnameverification.net – for TLDs registered by our registrar associate, Gandi. To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

When you receive the verification email, choose the link in the email that verifies that the email address is valid. If you don't receive the email immediately:

- Check the settings for the domain to verify that you specified the correct email address for the registrant contact.

- Check your junk email folder.

Important

The registrant contact must follow the instructions in the email to confirm that the email was received, or we must suspend the domain as required by ICANN. When a domain is suspended, it's not accessible on the internet.

13. For all TLDs, you'll receive an email when your domain registration has been approved.

To determine the current status of your request, see [Viewing the status of a domain registration \(p. 52\)](#).

14. (Optional) The domain registries for all generic TLDs and many geographic TLDs let you lock a domain to prevent someone from transferring the domain to another registrar without your permission. To determine whether the registry for your domain lets you lock the domain, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#). If locking is supported and you want to lock your domain, see [Locking a domain to prevent unauthorized transfer to another registrar \(p. 59\)](#).

15. When domain registration is complete, your next step depends on whether you want to use Route 53 or another DNS service as the DNS service for the domain:

- **Route 53** – In the hosted zone that Route 53 created when you registered the domain, create records to tell Route 53 how you want to route traffic for the domain and subdomains.

For example, when someone enters your domain name in a browser and that query is forwarded to Route 53, do you want Route 53 to respond to the query with the IP address of a web server in your data center or with the name of an ELB load balancer?

For more information, see [Working with records \(p. 370\)](#).

Important

If you create records in a hosted zone other than the one that Route 53 creates automatically, you must update the name servers for the domain to use the name servers for the new hosted zone.

- **Another DNS service** – Configure your new domain to route DNS queries to the other DNS service. Perform the procedure [To update the name servers for your domain when you want to use another DNS service \(p. 46\)](#).

To update the name servers for your domain when you want to use another DNS service

1. Use the process that is provided by your DNS service to get the name servers for the domain.
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Registered Domains**.
4. Choose the name of the domain that you want to configure to use another DNS service.
5. Choose **Add/Edit Name Servers**.
6. Change the names of the name servers to the name servers that you got from your DNS service in step 1.
7. Choose **Update**.
8. (Optional) Delete the hosted zone that Route 53 created automatically when you registered your domain. This prevents you from being charged for a hosted zone that you aren't using.
 - a. In the navigation pane, choose **Hosted Zones**.
 - b. Select the radio button for the hosted zone that has the same name as your domain.
 - c. Choose **Delete Hosted Zone**.

- d. Choose **Confirm** to confirm that you want to delete the hosted zone.

Values that you specify when you register or transfer a domain

When you register a domain or transfer domain registration to Amazon Route 53, you specify the values that are described in this topic.

Note

If you're registering more than one domain, Route 53 uses the values that you specify for all of the domains that are in your shopping cart.

You can also change values for a domain that is currently registered with Route 53. Note the following:

- If you change contact information for the domain, we send an email notification to the registrant contact about the change. This email comes from route53-dev-admin@amazon.com. For most changes, the registrant contact is not required to respond.
- For changes to contact information that also constitute a change in ownership, we send the registrant contact an additional email. ICANN requires that the registrant contact confirm receiving the email. For more information, see **First Name, Last Name** and **Organization** later in this section.

For more information about changing settings for an existing domain, see [Updating settings for a domain \(p. 52\)](#).

Values That You Specify

- [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 \(Only available when editing domain settings\)](#)

My Registrant, Administrative, and Technical contacts are all the same

Specifies whether you want to use the same contact information for the registrant of the domain, the administrative contact, and the technical contact.

Contact Type

Category for this contact. Note the following:

- If you choose an option other than **Person**, you must enter an organization name.
- For some TLDs, the privacy protection available depends on the value that you choose for **Contact Type**. For the privacy protection settings for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).
- For .es domains, the value of **Contact Type** must be **Person** for all three contacts.

First Name, Last Name

The first and last names of the contact.

Important

For **First Name** and **Last Name**, we recommend that you specify the name on your official ID. For some changes to domain settings, you must provide proof of identity, and the name on your ID must match the name of the registrant contact for the domain.

If you're transferring a domain to Route 53 and the following are true, then you're changing the owner of the domain:

- The contact type is **Person**.
- You're changing the **First Name** and/or **Last Name** fields for the registrant contact from the current settings.

In that case, ICANN requires that we email the registrant contact to get approval. The email comes from one of the following email addresses:

TLDs	Email address that approval email comes from
TLDs registered by Amazon Registrar	noreply@registrar.amazon.com
.fr	nic@nic.fr (The email is sent both to the current registrant contact and the new registrant contact.)
All others	noreply@domainnameverification.net

To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Important

The registrant contact must follow the instructions in the email to confirm that the email was received, or we must suspend the domain as required by ICANN. When a domain is suspended, it's not accessible on the internet.

If you change the email address of the registrant contact, this email is sent to the former email address and the new email address for the registrant contact.

Some TLD registrars charge a fee for changing the domain owner. When you change one of these values, the Route 53 console displays a message that tells you whether there is a fee.

Organization

The organization that is associated with the contact, if any. For the registrant and administrative contacts, this is typically the organization that is registering the domain. For the technical contact, this might be the organization that manages the domain.

When the contact type is any value except **Person** and you change the **Organization** field for the registrant contact, you change the owner of the domain. ICANN requires that we email the registrant contact to get approval. The email comes from one of the following email addresses:

TLDs	Email address that approval email comes from
TLDs registered by Amazon Registrar	noreply@registrar.amazon.com
.fr	nic@nic.fr (The email is sent both to the current registrant contact and the new registrant contact.)
All others	noreply@domainnameverification.net

To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

If you change the email address of the registrant contact, this email is sent to the former email address and the new email address for the registrant contact.

Some TLD registrars charge a fee for changing the domain owner. When you change the value of **Organization**, the Route 53 console displays a message that tells you whether there is a fee.

Email

The email address for the contact.

If you change the email address for the registrant contact, we send a notification email to the former email address and the new email address. This email comes from route53-dev-admin@amazon.com.

Phone

The phone number for the contact:

- If you're entering a phone number for locations in the United States or Canada, enter **1** in the first field and the 10-digit area code and phone number in the second field.
- If you're entering a phone number for any other location, enter the country code in the first field, and enter the rest of the phone number in the second field. For a list of phone country codes, see the Wikipedia article [List of country calling codes](#).

Address 1

The street address for the contact.

Address 2

Additional address information for the contact, for example, apartment number or mail stop.

Country

The country for the contact.

State

The state or province for the contact, if any.

City

The city for the contact.

Postal/Zip Code

The postal or zip code for the contact.

Fields for selected top-level domains

The following top-level domains (TLDs) require that you specify additional values:

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

In addition, many TLDs require a VAT identification number.

For information about valid values, see [ExtraParam](#) in the *Amazon Route 53 API Reference*.

Privacy Protection

Whether you want to conceal your contact information from WHOIS queries. If you select **Hide contact information**, WHOIS ("who is") queries will return contact information for the registrar or the value "Protected by policy."

Note

You must specify the same privacy setting for the administrative, registrant, and technical contacts.

If you select **Don't hide contact information**, you'll get more email spam at the email address that you specified.

Anyone can send a WHOIS query for a domain and get back all of the contact information for that domain. The WHOIS command is available in many operating systems, and it's also available as a web application on many websites.

Important

Although there are legitimate users for the contact information associated with your domain, the most common users are spammers, who target domain contacts with unwanted email and bogus offers. In general, we recommend that you choose **Hide contact information** for **Privacy Protection**.

To enable or disable privacy protection for some domains, you must open a support case and request privacy protection.

For more information about privacy protection, see the following topics:

- [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#)
- [Domains that you can register with Amazon Route 53 \(p. 97\)](#)

Auto Renew (Only available when editing domain settings)

Whether you want Route 53 to automatically renew the domain before it expires. The registration fee is charged to your AWS account. For more information, see [Renewing registration for a domain \(p. 63\)](#).

Important

If you disable automatic renewal, registration for the domain will not be renewed when the expiration date passes, and you might lose control of the domain name.

The period during which you can renew a domain name varies by top-level domain (TLD). For an overview about renewing domains, see [Renewing registration for a domain \(p. 63\)](#). For

information about extending domain registration for a specified number of years, see [Extending the registration period for a domain \(p. 59\)](#).

Values that Amazon Route 53 returns when you register a domain

When you register your domain with Amazon Route 53, Route 53 returns the following values in addition to the values that you specified.

Registered on

The date on which the domain was originally registered with Route 53.

Expires on

The date and time on which the current registration period expires, in Greenwich Mean Time (GMT).

The registration period is typically one year, although the registries for some top-level domains (TLDs) have longer registration periods. For the registration and renewal period for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

For most TLDs, you can extend the registration period by up to ten years. For more information, see [Extending the registration period for a domain \(p. 59\)](#).

Domain name status code

The current status of the domain.

ICANN, the organization that maintains a central database of domain names, has developed a set of domain name status codes (also known as EPP status codes) that tell you the status of a variety of operations on a domain name, for example, registering a domain name, transferring a domain name to another registrar, renewing the registration for a domain name, and so on. All registrars use this same set of status codes.

For a current list of domain name status codes and an explanation of what each code means, go to the [ICANN website](#) and search for **epp status codes**. (Search on the ICANN website; web searches sometimes return an old version of the document.)

Transfer lock

Whether the domain is locked to reduce the possibility of someone transferring your domain to another registrar without your permission. If the domain is locked, the value of **Transfer Lock** is **Enabled**. If the domain is not locked, the value is **Disabled**.

Auto renew

Whether Route 53 will automatically renew the registration for this domain shortly before the expiration date.

Authorization code

The code that is required if you want to transfer registration of this domain to another registrar. An authorization code is only generated when you request it. For information about transferring a domain to another registrar, see [Transferring a domain from Amazon Route 53 to another registrar \(p. 83\)](#).

Name servers

The Route 53 servers that respond to DNS queries for this domain. We recommend that you don't delete Route 53 name servers.

For information about adding, changing, or deleting name servers, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#).

Viewing the status of a domain registration

ICANN, the organization that maintains a central database of domain names, has developed a set of domain name status codes (also known as EPP status codes) that tell you the status of a variety of operations, for example, registering a domain name, transferring a domain name to another registrar, renewing the registration for a domain name, and so on. All registrars use this same set of status codes.

To view the status code for your domains, perform the following procedure.

To view the status of a domain

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Select the linked name of your domain.
4. For the current status of your domain, see the value of the **Domain name status** field.

For a current list of domain name status codes and an explanation of what each code means, go to the [ICANN website](#) and search for **epp status codes**. (Search on the ICANN website; web searches sometimes return an old version of the document.)

Updating settings for a domain

For information about updating settings for a domain, see the applicable topic.

Topics

- [Updating contact information and ownership for a domain \(p. 52\)](#)
- [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#)
- [Enabling or disabling automatic renewal for a domain \(p. 59\)](#)
- [Locking a domain to prevent unauthorized transfer to another registrar \(p. 59\)](#)
- [Extending the registration period for a domain \(p. 59\)](#)
- [Adding or changing name servers and glue records for a domain \(p. 61\)](#)

Updating contact information and ownership for a domain

For the administrative and technical contacts for a domain, you can change all contact information without having to authorize the changes. For more information, see [Updating contact information for a domain \(p. 54\)](#).

For the registrant contact, you can change most values without having to authorize the changes. However, for some TLDs, changing the owner of a domain requires authorization. For more information, see the applicable topic.

Topics

- [Who is the owner of a domain? \(p. 53\)](#)
- [TLDs that require special processing to change the owner \(p. 53\)](#)
- [Updating contact information for a domain \(p. 54\)](#)
- [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#)

Who is the owner of a domain?

When the contact type is **Person** and you change the **First Name** or **Last Name** fields for the registrant contact, you change the owner of the domain.

When the contact type is any value except **Person** and you change **Organization**, you change the owner of the domain.

Note the following about changing the owner of a domain:

- For some TLDs, there's a fee to change the owner of a domain. To determine whether there's a fee for the TLD for your domain, see the "Change Ownership Price" column in [Amazon Route 53 Pricing for Domain Registration](#).

Note

You can't use AWS credits to pay the fee, if any, to change the owner of a domain.

- For some TLDs, when you change the owner of a domain, we send an authorization email to the email address for the registrant contact. The registrant contact must follow the instructions in the email to authorize the change.
- For some TLDs, you need to fill out a Change of Domain Ownership Form and provide proof of identity so that an Amazon Route 53 support engineer can update the values for you. If the TLD for your domain requires a Change of Domain Ownership form, the console displays a message that links to a form for opening a support case. For more information, see [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

TLDs that require special processing to change the owner

When you change the owner of a domain, the registries for some TLDs require special processing. If you're changing the owner for any of the following domains, perform the applicable procedure. If you're changing the owner for any other domain, you can change the owner yourself, either programmatically or using the Route 53 console. See [Updating contact information for a domain \(p. 54\)](#).

The following TLDs require special processing to change the owner of the domain:

.be, .cl, .com.br, .com.sg, .es, .fi, .im, .it, .ru, .se, .sg, .sh

.be

You must get a transfer code from the registry for .be domains, and then open a case with AWS Support.

- To get the transfer code, see <https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer>, and follow the prompts.
- To open a case, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

.cl

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.com.ar

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.com.br

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.com.sg

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.es

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.fi

You must open a case with AWS Support. See [Contacting AWS Support about domain registration issues \(p. 95\)](#).

.im

You must open a case with AWS Support. See [Contacting AWS Support about domain registration issues \(p. 95\)](#).

.it

You must open a case with AWS Support. See [Contacting AWS Support about domain registration issues \(p. 95\)](#).

.qa

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.ru

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.se

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.sg

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

.sh

You must complete and submit a form to AWS Support. See [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#).

Updating contact information for a domain

To update contact information for a domain, perform the following procedure.

To update contact information for a domain

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain that you want to update contact information for.
4. Choose **Edit Contacts**.
5. If you're changing the email address for the registrant contact, perform the following steps. If you aren't changing the email address for the registrant contact, skip to step 6.
 - a. Choose the **Registrant Contact** tab.
 - b. Under **Contact Information**, choose **Change**.
 - c. Enter the new email address in the **Email Address** field.
 - d. Choose **Save Changes**.

- a. Change *only* the email address for the registrant contact. Don't change any other values for any of the contacts for the domain. If you also want to change other values, you change them later in the process.

Choose **Save**.

If the new email address is an address that you have never verified is reachable, we send email to the new email address. You must choose the link in the email to verify that the new email address is valid. If you don't verify the new email address, Route 53 suspends the domain as required by ICANN.

- b. If you want to change other values for the registrant, administrative, or technical contacts for the domain, return to step 1 and repeat the procedure.
6. Update the applicable values. For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

Depending on the TLD for your domain and the values that you're changing, the console might display the following message:

"To change the registrant name or organization, open a case."

If you see that message, skip the rest of this procedure and see [Changing the owner of a domain when the registry requires a Change of Domain Ownership form \(p. 56\)](#) for more information.

7. Choose **Save**.
8. **AISPL (India) customers only:** If your contact address is in India, your user agreement is with Amazon Internet Services Pvt. Ltd (AISPL), a local AWS seller in India. To change the owner of a domain when the TLD registry charges a fee to change the owner, perform the following steps to pay the fee for the extension.
 - a. Go to the [Orders and Invoices](#) page in the AWS Management Console.
 - b. In the **Payments Due** section, find the applicable invoice.
 - c. In the **Actions** column, choose **Verify and Pay**.

After you pay the invoice, we change the applicable settings for the registrant contact.

Important

If you don't pay the invoice within five days, the invoice is canceled. To change settings for the registrant contact after an invoice is canceled, resubmit the request.

For more information, see [Managing your payments in India](#) in the *AWS Billing and Cost Management User Guide*.

9. If you changed the domain owner, as described in [Who is the owner of a domain? \(p. 53\)](#), we send email to the registrant contact for the domain. The email asks for authorization for the change of owner.

If we don't receive authorization for the change within 3 to 15 days, depending on the top-level domain, we must cancel the request as required by ICANN.

The email comes from one of the following email addresses.

TLDs	Email address that authorization email comes from
.fr	nic@nic.fr
.com.au	noreply@emailverification.info

TLDs	Email address that authorization email comes from
.net.au	
All others	One of the following email addresses: <ul style="list-style-type: none">• noreply@registrar.amazon.com• noreply@domainnameverification.net

10. If you encounter issues while updating contact information, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

For information about the API you can use also, see [UpdateDomainContact](#).

Changing the owner of a domain when the registry requires a Change of Domain Ownership form

If the registry for your domain requires you to complete a Change of Domain Ownership and submit the form to AWS Support, perform the following procedure. To determine whether you need to perform this procedure, see the following topics:

- To determine whether the value you're changing is considered a change of owner, see [Who is the owner of a domain? \(p. 53\)](#).
- To determine whether a Change of Domain Ownership form is required for your domain, see [TLDs that require special processing to change the owner \(p. 53\)](#).

To change the owner of a domain when the registry requires a Change of Domain Ownership form

1. See the introduction to this topic to determine whether the registry for your domain requires special processing to change the owner of the domain. If so, and if a Change of Domain Ownership form is required, continue with this procedure.

If no Change of Domain Ownership form is required, perform the procedure in the applicable topic instead.

2. Download the [Change of Domain Ownership Form](#). The file is compressed into a .zip file.
3. Fill out the form.
4. For the registrant contact for the former owner of the domain *and* for the new owner, get a copy of a signed proof of identity (identity card, driver's license, passport, or other legal proof of identity).

In addition, if a legal entity is listed as the registrant organization, gather the following information for the former owner of the domain *and* for the new owner:

- Proof that the organization that the domain is registered to exists.
 - Proof that the representatives for the former owner and the new owner are authorized to act on the organization's behalf. This document must be a certified legal document that contains both the name of the organization and the names of the representatives as signing officers (for example, CEO, President, or Executive Director).
5. Scan the Change of Domain Ownership form and the required proof. Save the scanned documents in a common format, such as a .pdf file or a .png file.
 6. Using the AWS account that the domain is currently registered to, sign in to the [AWS Support Center](#).

Important

You must sign in either by using the root account or by using an IAM user that has been granted IAM permissions in one or more of the following ways:

- The user is assigned the **AdministratorAccess** managed policy.
- The user is assigned the **AmazonRoute53DomainsFullAccess** managed policy.
- The user is assigned the **AmazonRoute53FullAccess** managed policy.

If you don't sign in either by using the root account or by using an IAM user that has the required permissions, we can't update the domain owner. This requirement prevents unauthorized users from changing the owner of a domain.

7. Specify the following values:

Regarding

Accept the default value of **Account and Billing Support**.

Service

Accept the default value of **Billing**.

Category

Accept the default value of **Domain name registration issue**.

Subject

Specify **Change the owner of a domain**.

Description

Provide the following information:

- Domain that you want to change the owner for
- **12-digit account ID** of the AWS account that the domain is registered to

Add attachment

Upload the documents that you scanned in step 5.

Contact method

Specify a contact method and enter the applicable values.

8. Choose **Submit**.

An AWS Support engineer reviews the information that you provided and updates the settings. The engineer will either contact you when the update is finished or contact you for more information.

Enabling or disabling privacy protection for contact information for a domain

When you register a domain with Amazon Route 53 or transfer a domain to Route 53, we enable privacy protection by default for all the contacts for the domain. This typically hides most of your contact information from WHOIS ("Who is") queries and reduces the amount of spam that you receive. Your contact information is replaced either with contact information for the registrar or with the phrase "REDACTED FOR PRIVACY."

If you choose to disable privacy protection, you must disable it for all contacts for a domain. If you do disable privacy protection, anyone can query WHOIS for the domain and, for most top-level

domains (TLDs), might be able to get all the contact information that you provided when you registered or transferred the domain, including name, address, phone number, and email address. The WHOIS command is widely available; it's included in many operating systems, and it's also available as a web application on many websites.

The information that you can hide from WHOIS queries depends on two main factors:

The registry for the top level domain

Most TLD registries hide all contact information automatically, some allow you to choose to hide all contact information, some allow you to hide only some information, and some do not allow you to hide any information.

Note

To enable or disable privacy protection for some domains, you must open a support case and request privacy protection. For more information, see the applicable section in [Domains that you can register with Amazon Route 53 \(p. 97\)](#):

- [.co.uk \(United Kingdom\)](#)
- [.me.uk \(United Kingdom\)](#)
- [.org.uk \(United Kingdom\)](#)
- [.link](#)

The registrar

When you register a domain with Route 53 or transfer a domain to Route 53, the registrar for the domain is either Amazon Registrar or our registrar associate, Gandi. Amazon Registrar and Gandi hide different information by default:

- **Amazon Registrar** – By default, all of your contact information is hidden. However, regulations for the TLD registry take precedence.
- **Gandi** – By default, all of your contact information is hidden except organization name, if any. However, regulations for the TLD registry take precedence.

For [geographic TLDs](#) that don't allow privacy protection, your personal information will be marked as "redacted" on the [Whois Directory Search](#) page on the Gandi website. However, your personal information might be available at the domain registry or on third-party WHOIS websites.

To find out what information is hidden for the TLD for your domain, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

When you want to enable or disable privacy protection for a domain that you registered using Route 53, perform the following procedure.

To enable or disable privacy protection for contact information for a domain

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain that you want to enable or disable privacy protection for.
4. Choose **Edit Contacts**.
5. Choose whether to hide contact information. You must specify the same privacy setting for all three contacts: administrative, registrant, and technical.
6. Choose **Save**.
7. If you encounter issues while enabling or disabling privacy protection, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Enabling or disabling automatic renewal for a domain

When you want to change whether Amazon Route 53 automatically renews registration for a domain shortly before the expiration date, or you want to see the current setting for automatic renewal, perform the following procedure.

Note that you can't use AWS credits to pay the fee for renewing registration for a domain.

To enable or disable automatic renewal for a domain

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain that you want to update.
4. Choose **Enable** (to turn on automatic renewal) or **Disable** (to turn off automatic renewal).
5. If you encounter issues while enabling or disabling automatic renewal, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Locking a domain to prevent unauthorized transfer to another registrar

The domain registries for all generic TLDs and many geographic TLDs let you lock a domain to prevent someone from transferring the domain to another registrar without your permission. To determine whether the registry for your domain lets you lock the domain, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#). If locking is supported and you want to lock your domain, perform the following procedure. You can also use the procedure to disable the lock if you want to transfer a domain to another registrar.

To lock a domain to prevent unauthorized transfer to another registrar

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain that you want to update.
4. Choose **Enable** (to lock the domain) or **Disable** (to unlock the domain).
5. Choose **Save**.
6. If you encounter issues while locking a domain, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

In WHOIS search this status shows up as: `clientTransferProhibited`.

Extending the registration period for a domain

When you register a domain with Amazon Route 53 or you transfer domain registration to Route 53, we configure the domain to renew automatically. The automatic renewal period is typically one year, although the registries for some top-level domains (TLDs) have longer renewal periods.

Note the following:

Maximum renewal period

All generic TLDs and many country-code TLDs let you extend domain registration for longer periods, typically up to ten years in one-year increments. To determine whether you can extend the registration period for your domain, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#). If longer registration periods are allowed, perform the following procedure.

Restrictions on when you can renew or extend a domain registration

Some TLD registries have restrictions on when you can renew or extend a domain registration, for example, the last two months before the domain expires. Even if the registry allows extending the registration period for a domain, they might not allow it at the current number of days before the domain expires.

AWS credits

You can't use AWS credits to pay the fee for extending the registration period for a domain.

To extend the registration period for your domain

1. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain for which you want to extend the registration period.

The **Expires on** field lists the current expiration date for the domain. If the registry for the TLD allows extending the registration period, an **extend** link appears on the right side of the expiration date.

4. Choose **extend**.
5. In the **Extend registration for** list, choose the number of years that you want to extend the registration for.

The list shows all the current options based on the current expiration date and the maximum registration period allowed by the registry for this domain. The **New expiration date** field shows the expiration date with that number of years applied.

6. Choose **Extend domain registration**.

When we receive confirmation from the registry that they've updated your expiration date, we send you an email to confirm that we've changed the expiration date.

7. **AISPL (India) customers only:** If your contact address is in India, your user agreement is with Amazon Internet Services Pvt. Ltd (AISPL), a local AWS seller in India. To extend the registration for a domain, perform the following steps to pay the fee for the extension.
 - a. Go to the [Orders and Invoices](#) page in the AWS Management Console.
 - b. In the **Payments Due** section, find the applicable invoice.
 - c. In the **Actions** column, choose **Verify and Pay**.

After you pay the invoice, we complete the extension and send the applicable emails.

Important

If you don't pay the invoice within five days, the invoice is canceled. To extend the domain registration after an invoice is canceled, resubmit the request.

For more information, see [Managing your payments in India](#) in the *AWS Billing and Cost Management User Guide*.

8. If you encounter issues while extending the registration period for a domain, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Adding or changing name servers and glue records for a domain

When you register a domain with Route 53, we automatically create a hosted zone for the domain, assign four name servers to the hosted zone, and then update the domain registration to use those name servers. You typically don't need to change those settings unless you want to use another DNS service or you want to use white-label name servers.

The maximum number of nameservers per domain in Route 53 is 6.

Warning

If you change name servers to the wrong values, specify the wrong IP addresses in glue records, or delete one or more name servers without specifying new ones, your website or application might become unavailable on the internet for up to two days.

Topics

- [Considerations for changing name servers and glue records \(p. 61\)](#)
- [Adding or changing name servers or glue records \(p. 62\)](#)

Considerations for changing name servers and glue records

Consider the following issues before you change your configuration.

Topics

- [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](#)

You want to make Route 53 the DNS service for your domain

If you're currently using another DNS service and you want to make Route 53 the DNS service for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#) for detailed instructions on how to migrate DNS service to Route 53.

Important

If you don't rigorously follow the migration process, your domain can become unavailable on the internet for up to two days.

You want to use another DNS service

If you want to use a DNS service other than Route 53 for your domain, use the following procedure to change the name servers for the domain registration to the name servers that are provided by the other DNS service.

Note

If you change name servers and Route 53 returns the following error message, the registry for the TLD doesn't recognize the name servers that you specified as valid name servers:

"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 nameservers are not known to the domain registry." TLD registries commonly support name servers provided by public DNS services but don't support private DNS servers, such as DNS servers that you configured on Amazon EC2 instances, unless the registry has IP addresses for those name servers. Route 53 doesn't

support using name servers that aren't recognized by the TLD registry. If you encounter this error, you must change to name servers for Route 53 or another public DNS service.

You want to use white-label name servers

If you want the names of your name servers to be subdomains of your domain name, you can create white-label name servers. (White-label name servers are also known as vanity name servers or private name servers.) For example, you might create name servers ns1.example.com through ns4.example.com for the domain example.com. To use white-label name servers, use the following procedure to specify the IP addresses of your name servers instead of the names. These IP addresses are known as glue records.

For more information about configuring white-label name servers, see [Configuring white-label name servers \(p. 349\)](#).

You're changing name servers for a .it domain

If you change name servers for a .it domain, the registry for .it domains performs a check to confirm that the name servers are valid. If you specify the wrong name servers and the check fails, the registry continues to check for 22 days. During this time, you can't update the names of the name servers to correct the error because the EPP status code is pendingUpdate. The registry continues to respond to DNS queries using the name servers from before you made the change. If the previous name servers are no longer available, your domain becomes unavailable on the internet.

Important

Whenever you change name servers for a domain, confirm that DNS is responding to queries with the new name servers before you cancel the old DNS service or you delete the Route 53 hosted zone that used the old name servers.

For information about getting help from AWS to correct the names of your name servers with the registry for .it domains, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Adding or changing name servers or glue records

To add or change name servers or glue records, perform the following procedure.

Note

By default, DNS resolvers typically cache the names of name servers for two days. As a result, your changes can take two days to take effect. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

To add or change name servers or glue records for a domain

1. Review [Considerations for changing name servers and glue records \(p. 61\)](#) and address the applicable issues, if any.
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Registered Domains**.
4. Choose the name of the domain for which you want to edit settings.
5. Choose **Add/Edit Name Servers**.
6. In the **Edit Name Servers** dialog box, you can do the following:
 - Change the DNS service for the domain by doing one of the following:
 - Replace the name servers for another DNS service with the name servers for a Route 53 hosted zone
 - Replace the name servers for a Route 53 hosted zone with the name servers for another DNS service

- Replace the name servers for one Route 53 hosted zone with the name servers for a different Route 53 hosted zone

For information about changing the DNS service for a domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#). For information about getting the name servers for the Route 53 hosted zone that you want to use for DNS service for the domain, see [Getting the name servers for a public hosted zone \(p. 341\)](#).

- Add one or more name servers.
- Replace the name of an existing name server.
- If you specify white-label name servers, add or change the IP addresses in glue records. You can enter addresses in IPv4 or IPv6 format. If a name server has multiple IP addresses, enter each address on a separate line.

A white-label name server includes your domain name, such as example.com, in the name of the name server, such as ns1.example.com. When you specify a white-label name server, Route 53 prompts you to specify one or more IP addresses for the name server. The IP address is known as a glue record. For more information, see [Configuring white-label name servers \(p. 349\)](#).

- Delete a name server. Choose the x icon on the right side of the field for that name server.

Warning

If you change name servers to the wrong values, specify the wrong IP addresses in glue records, or delete one or more name servers without specifying new ones, your website or application might become unavailable on the internet for up to two days.

7. Choose **Update**.
8. If you encounter issues while adding or changing name servers or glue records, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Renewing registration for a domain

When you register a domain with Amazon Route 53 or you transfer domain registration to Route 53, we configure the domain to renew automatically. The automatic renewal period is typically one year, although the registries for some top-level domains (TLDs) have longer renewal periods. For the registration and renewal period for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Note

You can't use AWS credits to pay the fee for renewing registration for a domain.

For most top-level domains (TLDs), you can change the expiration date for a domain. For more information, see [Extending the registration period for a domain \(p. 59\)](#).

Important

If you turn off automatic renewal, be aware of the following effects on your domain:

- Some TLD registries delete domains even before the expiration date if you don't renew early enough. We strongly recommend that you leave automatic renewal enabled if you want to keep a domain name.
- We also strongly recommend that you don't plan to re-register a domain after it has expired. Some registrars allow others to register domains immediately after the domains expire, so you might not be able to re-register before the domain is taken by someone else.
- Some registries charge a large premium to restore expired domains.
- On or near the expiration date, the domain becomes unavailable on the internet.

To determine whether automatic renewal is enabled for your domain, see [Enabling or disabling automatic renewal for a domain \(p. 59\)](#).

If automatic renewal is enabled, here's what happens:

45 days before expiration

We send an email to the registrant contact that tells you that automatic renewal is currently enabled and gives instructions about how to disable it. Keep your registrant contact email address current so you don't miss this email.

35 or 30 days before expiration

For all domains except .com.ar, .com.br, and .jp domains, we renew domain registration 35 days before the expiration date so we have time to resolve any issues with your renewal before the domain name expires.

The registries for .com.ar, .com.br, and .jp domains require that we renew the domains no more than 30 days before expiration. You'll get a renewal email from Gandi, our registrar associate, 30 days before expiration, which is the same day that we renew your domain if you have automatic renewal enabled.

Note

When we renew your domain, we send you an email to let you know that we renewed it. If the renewal failed, we send you an email to explain why it failed.

If automatic renewal is disabled, here's what happens as the expiration date for a domain name approaches:

45 days before expiration

We send an email to the registrant contact for the domain that tells you that automatic renewal is currently disabled and gives instructions about how to enable it. Keep your registrant contact email address current so you don't miss this email.

30 days and 7 days before expiration

If automatic renewal is disabled for the domain, ICANN, the governing body for domain registration, requires the registrar to send you an email. The email comes from one of the following email addresses:

- noreply@registrar.amazon.com – For domains for which the registrar is Amazon Registrar.
- noreply@domainnameverification.net – For domains for which the registrar is our registrar associate, Gandi.

To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

If you enable automatic renewal less than 30 days before expiration, and the renewal period has not passed, we renew the domain within 24 hours.

Important

Some TLD registries stop allowing renewals as much as 25 days before the expiration date, and many don't allow renewal after the expiration date. In addition, processing a renewal can take up to a day. If you delay too long before enabling automatic renewal, the domain might expire before renewal can be processed, and you might lose the domain. If the expiration date is approaching, we recommend that you manually extend the expiration date for the domain. For more information, see [Extending the registration period for a domain \(p. 59\)](#).

For more information about renewal periods, see the "Deadlines for renewing and restoring domains" section for your TLD in [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

After the expiration date

Most domains are held by the registrar for a brief time after expiration, so you might be able to renew an expired domain after the expiration date, but we strongly recommend that you keep automatic renewal enabled if you want to keep your domain. For information about trying to renew a domain after the expiration date, see [Restoring an expired or deleted domain \(p. 65\)](#).

If your domain expires but late renewal is allowed for the domain, you can renew the domain for the standard renewal price. To determine whether a domain is still within the late-renewal period, perform the procedure in the [Extending the registration period for a domain \(p. 59\)](#) section. If the domain is still listed, it's within the late-renewal period.

For more information about renewal periods, see the "Deadlines for renewing and restoring domains" section for your TLD in [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Restoring an expired or deleted domain

If you don't renew a domain before the end of the late-renewal period or if you accidentally delete the domain, some registries for top-level domains (TLDs) allow you to restore the domain before it becomes available for others to register.

When a domain is deleted or it passes the end of the late-renewal period, it no longer appears in the Amazon Route 53 console.

Important

The price for restoring a domain is typically higher and sometimes much higher than the price for registering or renewing a domain. For the current price for restoring a domain, see the "Restoration Price" column in [Amazon Route 53 Pricing for Domain Registration](#).

You can't use AWS credits to pay the fee for restoring an expired domain.

To try to restore domain registration when a domain is deleted or the late-renewal period has expired

1. Determine whether the TLD registry for the domain supports restoring domains and, if so, the period during which restoration is allowed.
 - a. Go to [Domains that you can register with Amazon Route 53 \(p. 97\)](#).
 - b. Find the TLD for your domain, and review the values in the "Deadlines for renewing and restoring domains" section.

Important

We forward restoration requests to Gandi, which processes the requests during business hours Monday through Friday. Gandi is based in Paris, where the time is UTC/GMT +1 hour. As a result, depending on when you submit your request, in rare cases it can take a week or more for a request to be processed.

2. Review the price for restoring a domain, which is often higher and sometimes much higher than the price for registering or renewing a domain. In [Amazon Route 53 Pricing for Domain Registration](#), find the TLD for your domain (such as .com) and check the price in the "Restoration Price" column. If you still want to restore the domain, make note of the price; you'll need it in a later step.
3. Using the AWS account that the domain was registered to, sign in to the [AWS Support Center](#).
4. Specify the following values:

Regarding

Accept the default value of **Account and Billing Support**.

Service

Accept the default value of **Billing**.

Category

Accept the default value of **Domain name registration issue**.

Subject

Enter **Restore an expired domain** or **Restore a deleted domain**.

Description

Provide the following information:

- The domain that you want to restore
- The [12-digit account ID](#) of the AWS account that the domain was registered to
- Confirmation that you agree to the price for restoring the domain. Use the following text:

"I agree to the price of \$____ for restoring my domain."

Replace the blank with the price that you found in step 2.

Contact method

Specify a contact method and, if you choose **Phone**, enter the applicable values.

5. Choose **Submit**.
6. When we learn whether we were able to restore your domain, an AWS Support representative will contact you. In addition, if we were able to restore your domain, the domain will reappear in the console. The expiration date depends on whether the domain expired or was accidentally deleted:

The domain expired

The new expiration date is usually one or two years (depending on the TLD) after the old expiration date.

Note

The new expiration date is not calculated from the date that the domain was restored.

The domain was accidentally deleted

The expiration date typically doesn't change.

Replacing the hosted zone for a domain that is registered with Route 53

If you [delete the hosted zone](#) for a domain, you need to create another hosted zone when you're ready to make the domain available on the internet. Perform the following procedure.

To replace the hosted zone for a domain

1. Create a public hosted zone. For more information, see [Creating a public hosted zone \(p. 340\)](#).
2. Create records in the hosted zone. Records define how you want to route traffic for the domain (example.com) and subdomains (acme.example.com, zenith.example.com). For more information, see [Working with records \(p. 370\)](#).
3. Update the domain configuration to use the name servers for the new hosted zone. For more information, see [Adding or changing glue records for a domain \(p. 61\)](#).

Important

When you create a hosted zone, Route 53 assigns a set of four name servers to the hosted zone. If you delete a hosted zone and then create a new one, Route 53 assigns another set of four name servers. Typically, none of the name servers for the new hosted zone match any of the name servers for the previous hosted zone. If you don't update the domain configuration to use the name servers for the new hosted zone, the domain will remain unavailable on the internet.

4. If you encounter issues while replacing the hosted zone for a domain, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Transferring domains

You can transfer domain registration from another registrar to Amazon Route 53, from one AWS account to another, or from Route 53 to another registrar.

Topics

- [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#)
- [Viewing the status of a domain transfer \(p. 78\)](#)
- [How transferring a domain to Amazon Route 53 affects the expiration date for your domain registration \(p. 80\)](#)
- [Transferring a domain to a different AWS account \(p. 81\)](#)
- [Transferring a domain from Amazon Route 53 to another registrar \(p. 83\)](#)

Transferring registration for a domain to Amazon Route 53

To transfer the registration for a domain to Amazon Route 53, carefully follow the procedures in this topic.

Important

If you skip a step, your domain might become unavailable on the internet.

Note the following:

Contacting AWS Support

If you encounter issues while transferring a domain, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Expiration date

For information about how transferring your domain affects the current expiration date, see [How transferring a domain to Amazon Route 53 affects the expiration date for your domain registration \(p. 80\)](#).

Transfer fee

When you transfer a domain to Route 53, the transfer fee that we apply to your AWS account depends on the top-level domain, such as .com or .org. For more information, see [Route 53 Pricing](#).

You can't use AWS credits to pay the fee, if any, for transferring a domain to Route 53.

Note

Route 53 charges the fee for transferring your domain before we start the transfer process. If a transfer fails for some reason, we immediately credit your account for the cost of the transfer.

Special and premium domain names

TLD registries have assigned special or premium prices to some domain names. You can't transfer a domain to Route 53 if the domain has a special or premium price.

Domain quotas

The default maximum number of domains per AWS account is 20. You can [request a higher quota](#). For more information, see [Quotas on domains \(p. 672\)](#).

Nameservers limit

The maximum number of nameservers per domain in Route 53 is 6.

Topics

- [Transfer requirements for top-level domains \(p. 68\)](#)
- [Step 1: Confirm that Amazon Route 53 supports the top-level domain \(p. 69\)](#)
- [Step 2 \(optional\): Transfer your DNS service to Amazon Route 53 or another DNS service provider \(p. 69\)](#)
- [Step 3: Change settings with the current registrar \(p. 69\)](#)
- [Step 4: Get the names of your name servers \(p. 71\)](#)
- [Step 5: Request the transfer \(p. 71\)](#)
- [Step 6: AISPL \(India\) customers only: Pay the transfer fee \(p. 75\)](#)
- [Step 7: Click the link in the confirmation and authorization emails \(p. 76\)](#)
- [Step 8: Update the domain configuration \(p. 78\)](#)

Transfer requirements for top-level domains

Most domain registrars enforce requirements on transferring a domain to another registrar. The primary purpose of these requirements is to prevent the owners of fraudulent domains from repeatedly transferring the domains to different registrars. Requirements vary, but the following requirements are typical:

- You must have either registered the domain with the current registrar or transferred registration for the domain to the current registrar at least 60 days ago.
- If the registration for a domain name expired and had to be restored, it must have been restored at least 60 days ago.
- The domain cannot have any of the following domain name status codes:
 - clientTransferProhibited
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - serverTransferProhibited
- The registries for some top-level domains don't allow transfers until changes are complete, such as changes to the domain owner.

For a current list of domain name status codes and an explanation of what each code means, go to the [website for ICANN](#), and search for "EPP status codes". (Search on the ICANN website; web searches sometimes return an old version of the document.)

Note

ICANN is the organization that establishes policies governing registration and transfer of domain names.

You can also search for your domain name in [website for Whois](#) to see status codes and other information for your domain.

Step 1: Confirm that Amazon Route 53 supports the top-level domain

See [Domains that you can register with Amazon Route 53 \(p. 97\)](#). If the top-level domain for the domain that you want to transfer is on the list, you can transfer the domain to Amazon Route 53.

If a TLD is not on the list, you can't currently transfer the domain registration to Route 53. We occasionally add more TLDs to the list, so check back to see if we've added support for your domain. You can also submit a request for support for your TLD on the [Route 53 Domain Registration forum](#).

Step 2 (optional): Transfer your DNS service to Amazon Route 53 or another DNS service provider

Why transfer DNS first?

Some registrars provide free DNS service that might be disabled as soon as they receive a request from Route 53 to transfer the domain's registration. If you'd like Route 53 to provide DNS service for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Step 3: Change settings with the current registrar

Using the method provided by your current registrar, do each of the following for each domain that you want to 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 \(selected geographic TLDs\)](#)

Confirm that the email for the registrant contact for your domain is up to date

We'll send email to that email address to request authorization for the transfer. You need to click a link in the email to authorize the transfer. If you don't click the link, we must cancel the transfer.

Unlock the domain so it can be transferred

ICANN, the governing body for domain registrations, requires that you unlock your domain before you transfer it.

Confirm that the domain status allows you to transfer the domain

For more information, see [Transfer requirements for top-level domains \(p. 68\)](#).

Disable DNSSEC for the domain

If you use DNSSEC with a domain and you transfer the domain registration to Route 53, you must disable DNSSEC at the former registrar first. Then, after you transfer the domain registration,

take steps to set up DNSSEC for the domain in Route 53. Route 53 supports DNSSEC for domain registration and for DNSSEC signing. For more information, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

Important

If you transfer a domain registration to Route 53 while DNSSEC is configured, the DNSSEC public keys are transferred, too. If you transfer DNS service to a provider that doesn't support DNSSEC, DNS resolution fails intermittently until you delete the DNSSEC keys from the domain. For more information, see [Deleting public keys for a domain \(p. 92\)](#).

Get an authorization code

An authorization code from the current registrar authorizes us to request that registration for the domain be transferred to Route 53. You'll enter this code in the Route 53 console later in the process.

Some top-level domains have additional requirements:

.co.za domains

You don't need to get an authorization code to transfer a .co.za domain to Route 53.

.es domains

If you're transferring a .es domain to Route 53, you don't need to get an authorization code.

.jp domains

If you're transferring a .jp domain to Route 53, you don't need to get an authorization code.

.uk, .co.uk, .me.uk, and .org.uk domains

If you're transferring a .uk, .co.uk, .me.uk, or .org.uk domain to Route 53, you don't need to get an authorization code. Instead, use the method provided by your current domain registrar to update the value of the IPS tag for the domain to **GANDI**, all uppercase. (An IPS tag is required by Nominet, the registry for .uk domain names.) If your registrar doesn't provide a way to change the value of the IPS tag, [contact Nominet](#).

Note the following about changing the IPS tag:

You must request the transfer within five days

If you don't request the transfer within five days after you change the IPS tag, the tag changes back to the previous value. You must change the value of the IPS tag again, or the transfer request will fail.

Viewing the IPS tag in WHOIS queries

The change to the IPS tag doesn't appear in WHOIS queries until after the transfer to Route 53 has completed.

Email from Gandi

You might receive an email from our registrar associate, Gandi, about the transfer process. If you receive an email from Gandi (transfer-auth@gandi.net) about transferring your domain, ignore the instructions in the email because they aren't relevant to Route 53. Follow the instructions in this topic instead.

Renew your domain registration before you transfer the domain (selected geographic TLDs)

For most TLDs, when you transfer a domain, the registration is automatically extended by one year. However, for some geographic TLDs, registration is not extended when you transfer the domain. If you're transferring a domain to Route 53 that has one of these TLDs, we recommend that you renew the domain registration before you transfer the domain, especially if the expiration date is approaching.

Important

If you don't renew the domain before you transfer it, the registration could expire before the transfer is complete. If this happens, the domain becomes unavailable on the internet, and the domain name could become available for others to purchase.

Registration is not automatically extended when you transfer the following domains to another registrar:

- .ch (Switzerland)
- .cl (Chile)
- .co.uk (United Kingdom)
- .co.za (South Africa)
- .com.au (Australia)
- .cz (Czech Republic)
- .es (Spain)
- .fi (Finland)
- .im (Isle of Man)
- .jp (Japan)
- .me.uk (United Kingdom)
- .net.au (Australia)
- .org.uk (United Kingdom)
- .se (Sweden)
- .uk (United Kingdom)

Step 4: Get the names of your name servers

If you're using Amazon Route 53 as your DNS service or you're continuing to use the existing DNS service, we'll get the names of the name servers for you automatically later in the process. Skip to [Step 5: Request the transfer \(p. 71\)](#).

If you want to change the DNS service to a provider other than Route 53 at the same time that you're transferring the domain to Route 53, use the procedure provided by the DNS service provider to get the names of the name servers for each domain that you want to transfer.

Important

If the registrar for your domain is also the DNS service provider for the domain, transfer your DNS service to Route 53 or another DNS service provider *before* you continue with the process to transfer the domain registration.

If you transfer DNS service at the same time that you transfer domain registration, your website, email, and the web applications associated with the domain might become unavailable. For more information, see [Step 2 \(optional\): Transfer your DNS service to Amazon Route 53 or another DNS service provider \(p. 69\)](#).

Step 5: Request the transfer

To transfer domain registration from the current registrar to Amazon Route 53, use the Route 53 console to request the transfer. Route 53 handles the communication with the current registrar for the domain.

The procedure that you use depends on whether you want to transfer up to five domains or more than five domains:

- [To transfer domain registration to Route 53 for up to five domains \(p. 72\)](#)
- [To transfer domain registration to Route 53 for more than five domains \(p. 74\)](#)

Important

If you use the procedure to transfer more than five domains, Route 53 automatically configures the transferred domains to use the current DNS service for all the domains that you're transferring. If the registrar for your domain is also the DNS service provider for the domain and you don't transfer DNS service to another provider, your website, email, and the web applications associated with the domain might become unavailable. For more information, see [Step 2 \(optional\): Transfer your DNS service to Amazon Route 53 or another DNS service provider \(p. 69\)](#).

To transfer domain registration to Route 53 for up to five domains

1. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose **Transfer Domain**.
4. Enter the name of the domain for which you want to transfer registration to Route 53, and choose **Check**.
5. If the domain registration is available for transfer, choose **Add to cart**.

If the domain registration is not available for transfer, the Route 53 console lists the reasons. Contact your registrar for information about how to resolve the issues that prevent you from transferring the registration.

6. If you want to transfer other domain registrations, repeat steps 4 and 5.
7. When you've added all the domain registrations that you want to transfer, choose **Continue**.
8. For each domain name that you want to transfer, enter the applicable values:

Authorization code

Enter the authorization code that you got from your current registrar in [Step 3: Change settings with the current registrar \(p. 69\)](#).

Note

You don't need to enter an authorization code to transfer a .co.za, .es, .jp, .uk, .co.uk, .me.uk, or .org.uk domain to Route 53.

Name server options

Choose the applicable option:

- **Continue to use the name servers provided by the current registrar or DNS service** – If the current registrar for the domain is currently providing DNS service, we recommend that you transfer DNS service to another DNS service provider before you transfer the domain.

Important

Some registrars stop providing DNS service as soon as you request a transfer to another registrar. If the current registrar disables DNS service, your domain will become unavailable on the internet.

- **Import name servers from a Route 53 hosted zone that has the same name as the domain**
– When you select this option, the console displays a list of the hosted zones that have the same name as the domain. Choose the hosted zone that you want to use for routing traffic for the domain.
- **Specify new name servers to replace the current registrar's name servers (not recommended)** – If you're using a DNS service other than Route 53 for this domain, enter the names of the name servers that you got in [Step 4: Get the names of your name servers \(p. 71\)](#).

Important

We don't recommend choosing this option because transferring DNS service from one DNS service provider to another can take up to two days. The current registrar

might stop providing DNS service as soon as you request a transfer to another registrar. If the current registrar disables DNS service, your domain will become unavailable on the internet until the change to another DNS service provider takes effect.

Name servers

If you chose the option **Specify new name servers to replace the current registrar's name servers**, enter the names of the name servers that you got from the DNS service for the domain in [Step 4: Get the names of your name servers \(p. 71\)](#). By default, the **Name server** fields display the names of the current name servers for the domain.

Glue records

If the name of a name server is a subdomain of the domain that you're transferring (such as ns1.example.com in the domain example.com), enter one or more IP addresses for each name server. You can enter addresses in IPv4 or IPv6 format. If a name server has multiple IP addresses, enter each address on a separate line.

9. On the **Contact Details for Your n Domains** page, enter contact information for the domain registrant, administrator, and technical contact. The values that you enter here are applied to all the domains that you're transferring.

Important

We recommend that you specify the following values for the registrant contact (the domain owner):

- **First and last name:** We recommend that you specify the name that appears on your official ID. For some changes to domain settings, some domain registries require that you provide proof of identity. The name on your ID must match the name of the registrant contact for the domain.
- **Contact details:** During the domain transfer, we recommend that you specify the same values as are specified with the current registrar. When you change contact details for the registrant contact, you change the domain owner, and some TLD registries don't allow you to change the domain owner during a domain transfer. If you change contact details for the registrant contact, the transfer might fail. You can change contact details for the registrant contact after you transfer the domain.

By default, we use the same information for all three contacts. If you want to enter different information for one or more contacts, change the value of **My Registrant, Administrative, and Technical contacts are all the same to No.**

Note

For .it domains, the registrant and administrative contacts must be the same.

For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

10. For some TLDs, we're required to collect additional information. For these TLDs, enter the applicable values after the **Postal/Zip Code** field.
11. If the value of **Contact Type** is **Person**, choose whether you want to hide your contact information from WHOIS queries. For more information, see [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#).
12. Choose **Continue**.
13. Choose whether you want us to automatically renew your domain registration before the expiration date.

Note

Domain name registrations and renewals are not refundable. If you enable automatic domain renewal and you decide that you don't want the domain name after we renew the registration, you can't get a refund for the cost of the renewal.

14. Review the information you entered, read the terms of service, and select the check box to confirm that you've read the terms of service.
15. Choose **Complete Purchase**.

We confirm that the domain is eligible for transfer, and we send an email to the registrant contact for the domain to request authorization to transfer the domain.

To transfer domain registration to Route 53 for more than five domains

1. Open the Route 53 console at <https://console.aws.amazon.com/route53>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose **Transfer Domain**.
4. On the **Transfer domain to Route 53** page, choose **Transfer multiple domains to Route 53**.
5. For each domain that you want to transfer, enter the domain name and the authorization code in the following format. Note the comma between the domain name and the authorization code:

```
domain-name-1,authorization-code-1  
domain-name-2,authorization-code-2
```

If an authorization code isn't required for a domain, omit the comma, too:

```
domain-name-3
```

Note

You don't need to enter an authorization code to transfer a .co.za, .es, .jp, .uk, .co.uk, .me.uk, or .org.ukdomain to Route 53.

6. When you've entered all the domains that you want to transfer, choose **Continue**.
7. The **Check domain transferability** page lists the domains that you entered on the previous page and whether each domain can be transferred. You have the following options:

If all domains are transferable

Choose **Add transferable domains to cart**.

If one or more domains are untransferable and you want to transfer them

Review [Transfer requirements for top-level domains \(p. 68\)](#) to confirm that each untransferable domain meets the transfer requirements. If you don't find any obvious problems, contact the current registrar to determine why the domain can't be transferred to Route 53.

After you make any changes so that domains are transferable (for example, disabling the transfer lock), choose **Check transferability**, and Route 53 will repeat the transferability check.

If one or more domains are untransferable and you don't want to transfer them

Choose **Add transferable domains to cart**.

8. Choose **Continue**.
9. On the **Contact Details for Your n Domains** page, enter contact information for the domain registrant, administrator, and technical contact. The values that you enter here are applied to all the domains that you're transferring.

Important

We recommend that you specify the following values for the registrant contact (the domain owner):

- **First and last name:** We recommend that you specify the name that appears on your official ID. For some changes to domain settings, some domain registries require that you provide proof of identity. The name on your ID must match the name of the registrant contact for the domain.
- **Contact details:** During the domain transfer, we recommend that you specify the same values as are specified with the current registrar. When you change contact details for the registrant contact, you change the domain owner, and some TLD registries don't allow you to change the domain owner during a domain transfer. If you change contact details for the registrant contact, the transfer might fail. You can change contact details for the registrant contact after you transfer the domain.

By default, we use the same information for all three contacts. If you want to enter different information for one or more contacts, change the value of **My Registrant, Administrative, and Technical contacts are all the same to No.**

For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

10. For some TLDs, we're required to collect additional information. For these TLDs, enter the applicable values after the **Postal/Zip Code** field.
11. If the value of **Contact Type** is **Person**, choose whether you want to hide your contact information from WHOIS queries. For more information, see [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#).
12. Choose **Continue**.
13. Choose whether you want us to automatically renew your domain registration before the expiration date.

Note

Domain name registrations and renewals are not refundable. If you enable automatic domain renewal and you decide that you don't want the domain name after we renew the registration, you can't get a refund for the cost of the renewal.

14. Review the information you entered, read the terms of service, and select the check box to confirm that you've read the terms of service.
15. Choose **Complete Purchase**.

We confirm that the domain is eligible for transfer, and we send an email to the registrant contact for the domain to request authorization to transfer the domain.

Step 6: AISPL (India) customers only: Pay the transfer fee

If your contact address is in India, your user agreement is with Amazon Internet Services Pvt. Ltd (AISPL), a local AWS seller in India. To transfer a domain to Route 53, perform the following procedure to pay the fee for transferring your domain.

To pay the transfer fee

1. Go to the [Orders and Invoices](#) page in the AWS Management Console.
2. In the **Payments Due** section, find the applicable invoice.
3. In the **Actions** column, choose **Verify and Pay**.

After you pay the invoice, we complete the domain transfer and send the applicable emails.

Important

If you don't pay the invoice within five days, the invoice is canceled. To transfer a domain after an invoice is canceled, resubmit the request.

For more information, see [Managing your payments in India](#) in the *AWS Billing and Cost Management User Guide*.

Step 7: Click the link in the confirmation and authorization emails

Soon after you request the transfer, we might send one or more emails to the registrant contact for the domain:

Email to confirm that the registrant contact is reachable

If you've never registered a domain with Route 53 or transferred a domain to Route 53, we send you an email that asks you to confirm that the email address is valid. We retain this information so we don't have to send this confirmation email again.

Email to get authorization to transfer the domain

For some TLDs, you need to respond to an email to authorize transfer of the domain.

Generic TLDs such as .com, .net, and .org

Authorization isn't required for domains that have a [generic TLD](#), such as .com, .net, or .org.

Geographic TLDs such as .co.uk and .jp

For domains that have a [geographic TLD](#), we're required to get your authorization to transfer the domain. If you transfer 10 domains, we have to send you 10 emails, and you have to click the authorization link in each one.

The emails all go to the registrant contact for the domain:

- If you're the registrant contact for the domain, follow the instructions in the email to authorize the transfer.
- If someone else is the registrant contact, ask that person to follow the instructions in the email to authorize the transfer.

Important

If you're transferring a domain that has a geographic TLD, we wait up to five days for the registrant contact to authorize the transfer. If the registrant contact doesn't respond within five days, we cancel the transfer operation and send an email to the registrant contact about the cancellation.

Topics

- [Authorization email for a new owner or email address \(p. 76\)](#)
- [Email addresses that authorization emails come from \(p. 77\)](#)
- [Approval from the current registrar \(p. 77\)](#)
- [What happens next \(p. 77\)](#)

Authorization email for a new owner or email address

If you changed the following values, we send you a separate email that asks for your authorization:

Domain owner

If you change the owner of the domain, as described in [Who is the owner of a domain? \(p. 53\)](#), we send email to the registrant contact for the domain.

Email address for the registrant contact (only for some TLDs)

For some TLDs, if you change the email address for the registrant contact, we send an email to the old and the new email address for the registrant contact. Someone at both email addresses must follow the instructions in the email to authorize the change.

For changes to the domain owner or the email address for the registrant contact, if we don't receive authorization for the change within 3 to 15 days, depending on the top-level domain, we must cancel the request as required by ICANN.

Email addresses that authorization emails come from

All email comes from one of the following email addresses.

TLDs	Email address that authorization email comes from
.com.au and .net.au	no-reply@ispapi.net The email contains a link to http://transfers.ispapi.net .
.fr	nic@nic.fr, if you're changing the registrant contact for a .fr domain name at the same time that you're transferring the domain. (The email is sent both to the current registrant contact and the new registrant contact.)
All others	One of the following email addresses: <ul style="list-style-type: none">• noreply@registrar.amazon.com• noreply@domainnameverification.net

To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Approval from the current registrar

If the registrant contact authorizes the transfer, we start to work with your current registrar to transfer your domain. This step might take up to ten days, depending on the TLD for your domain:

- [Generic top-level domains \(p. 101\)](#) – take up to seven days
- [Geographic top-level domains \(p. 280\)](#) (also known as country code top-level domains) – take up to ten days

If your current registrar doesn't reply to our transfer request, which is common among registrars, the transfer happens automatically. If your current registrar rejects the transfer request, we send an email notification to the current registrant contact. The registrant needs to contact the current registrar and resolve the issues with the transfer.

What happens next

When your domain transfer has been approved, we send another email to the registrant contact. For more information about the process, see [Viewing the status of a domain transfer \(p. 78\)](#).

We charge your AWS account for the domain transfer as soon as the transfer is complete. For a list of charges by TLD, see [Amazon Route 53 Pricing for Domain Registration](#).

Note

This is a one-time charge, so the charge doesn't appear in your CloudWatch billing metrics. For more information about CloudWatch metrics, see [Using Amazon CloudWatch metrics](#) in the *Amazon CloudWatch User Guide*.

Step 8: Update the domain configuration

After the transfer is complete, you can optionally change the following settings:

Transfer lock

To transfer the domain to Route 53, you had to disable the transfer lock. If you want to re-enable the lock to prevent unauthorized transfers, see [Locking a domain to prevent unauthorized transfer to another registrar \(p. 59\)](#).

Automatic renewal

We configure the transferred domain to automatically renew as the expiration date approaches. For information about how to change this setting, see [Enabling or disabling automatic renewal for a domain \(p. 59\)](#).

Extended registration period

By default, Route 53 renews the domain annually. If you want to register the domain for a longer period, see [Extending the registration period for a domain \(p. 59\)](#).

DNSSEC

For information about configuring DNSSEC for the domain, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Viewing the status of a domain transfer

After you initiate the transfer of a domain from another domain registrar to Amazon Route 53, you can track the status on the **Pending requests** page of the Route 53 console. The **Status** column includes a brief description of the current step. The following list includes the text in the console and a more detailed description of each step.

Note

When you submit a transfer request, the initial status is **Domain transfer request submitted**, which indicates that we've received your request.

Determining whether the domain meets transfer requirements (step 1 of 14)

We're confirming that your domain's status is eligible for transfer. You must unlock your domain, and the domain can't have any of the following status codes when you submit the transfer request:

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

Geographic TLDs only – verifying WHOIS information (step 2 of 14)

If you're transferring a domain that has a [geographic TLD](#), we sent a WHOIS query for your domain to determine whether you've disabled the privacy protection for the domain. If privacy protection is still enabled with your current registrar, we won't be able to access the information we need to transfer the domain.

Note

Authorization isn't required for domains that have a [generic TLD](#), such as .com, .net, or .org.

Geographic TLDs only – Sent email to registrant contact to get transfer authorization (step 3 of 14)

If you're transferring a domain that has a [geographic TLD](#), we've sent an email to the registrant contact for the domain. The purpose of the email is confirm that the transfer was requested by an authorized contact of the domain.

Note

Authorization isn't required for domains that have a [generic TLD](#), such as .com, .net, or .org.

Verifying transfer with current registrar (step 4 of 14)

We've sent a request to the current registrar for the domain to initiate the transfer.

Geographic TLDs only – Awaiting authorization from registrant contact (step 5 of 14)

We sent email to the registrant contact for the domain (see step 3 of 14), and we're waiting for the registrant contact to click a link in the email to authorize the transfer. If you're transferring a domain that has a [geographic TLD](#) and you didn't receive the email for some reason, see [Resending authorization and confirmation emails \(p. 86\)](#).

Contacted current registrar to request transfer (step 6 of 14)

We're working with the current registrar for the domain to finalize the transfer.

Waiting for the current registrar to complete the transfer (step 7 of 14)

Your current registrar is confirming that your domain meets the requirements for being transferred. This step might take up to ten days, depending on the TLD for your domain:

- [Generic top-level domains \(p. 101\)](#) – take up to seven days
- [Geographic top-level domains \(p. 280\)](#) (also known as country code top-level domains) – take up to ten days

Note

If you have approved the confirmation email sent from Route 53 when transferring a .JP domain, but it has stopped for several days in STEP 7, contact [AWS Support Center](#) for assistance.

For most registrars, the process is entirely automated and can't be accelerated. Some registrars send you an email that asks you to approve the transfer; if your registrar sends this confirmation email, the transfer process might be much faster than seven to ten days.

For information about reasons that a registrar might reject the transfer, see [Transfer requirements for top-level domains \(p. 68\)](#).

Confirming with the registrant contact that the contact initiated the transfer (step 8 of 14)

Some TLD registries send the registrant contact another email to confirm that the domain transfer was requested by an authorized user.

Synchronizing name servers with the registry (step 9 of 14)

This step occurs only if the name servers that you provided as part of the transfer request are different from the name servers that are listed with the current registrar. We'll try to update your name servers to the new name servers that you provided.

Synchronizing settings with the registry (step 10 of 14)

We're verifying that the transfer has completed successfully, and we're synchronizing your domain-related data with our registrar associate.

Sending updated contact information to the registry (step 11 of 14)

If you changed the ownership of the domain when you requested the transfer, we're trying to make this change. However, most registries don't allow a transfer of ownership as part of the domain transfer process.

Finalizing the transfer to Route 53 (step 12 of 14)

We're confirming that the transfer process was successful.

Finalizing transfer (step 13 of 14)

We're setting up your domain in Route 53.

Transfer Complete (step 14 of 14)

Your transfer has been successfully completed.

How transferring a domain to Amazon Route 53 affects the expiration date for your domain registration

When you transfer a domain between registrars, some TLD registries let you keep the same expiration date for your domain, some registries add a year to the expiration date, and some registries change the expiration date to one year after the transfer date.

Note

For most TLDs, you can extend the registration period for a domain by up to ten years after you transfer it to Amazon Route 53. For more information, see [Extending the registration period for a domain \(p. 59\)](#).

Generic TLDs

When you transfer a domain that has a generic TLD (for example, .com) to Route 53, the new expiration date for the domain is the expiration date with your previous registrar plus one year.

Geographic TLDs

When you transfer a domain that has a geographic TLD (for example, .co.uk) to Route 53, the new expiration date for the domain depends on the TLD. Find your TLD in the following table to determine how transferring your domain affects the expiration date.

Continent	Geographic TLDs and the effect of transferring a domain on the expiration date
Africa	.co.za – The expiration date remains the same.
Americas	.cl, .com.ar, .com.br – The expiration date remains the same. .ca, .co, .mx, .us – One year is added to the old expiration date.
Asia/Oceania	.co.nz, .com.au, .com.sg, .jp, .net.au, .net.nz, .org.nz, .sg – The expiration date remains the same. .in – One year is added to the old expiration date.

Continent	Geographic TLDs and the effect of transferring a domain on the expiration date
Europe	<p>.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se – The expiration date remains the same.</p> <p>.berlin, .eu, .io, .me, .ruhr, .wien – One year is added to the old expiration date.</p> <p>.be, .de, .fr, .it, .nl – The new expiration date is one year after the date of transfer.</p>

Transferring a domain to a different AWS account

If you registered a domain using one AWS account and you want to transfer the domain to another AWS account, you can yourself using the AWS CLI or other programmatic methods.

Topics

- [Step 1: Transfer a domain to a different AWS account \(p. 81\)](#)
- [Step 2 \(Optional\): Migrate a hosted zone to a different AWS account \(p. 82\)](#)

Step 1: Transfer a domain to a different AWS account

When you want to transfer a domain from one AWS account to another, you have two options:

Transfer the domain yourself

You can transfer the domain yourself programmatically, using the AWS CLI, one of the AWS SDKs, or the Route 53 API. See the following documentation:

- For an overview of the transfer process and documentation about the API actions that you use to transfer a domain using the Route 53 domain registration API, see [TransferDomainToAnotherAwsAccount](#) in the *Amazon Route 53 API Reference*.
- For documentation about other options for transferring domains programmatically, see "SDKs & Toolkits" in the [Guides and API References](#) section of the "AWS documentation" page.

Important

When you transfer a domain to a different AWS account, either with help from AWS Support or programmatically, the hosted zone for the domain isn't transferred. If you also want to transfer the hosted zone, wait until the domain has been transferred, and then see [Step 2 \(Optional\): Migrate a hosted zone to a different AWS account \(p. 82\)](#).

To work with AWS Support to transfer a domain to a different AWS account

If you need help you can contact support as detailed in the following procedure. However, the self-serve method is the preferred way.

1. Using the AWS account that the domain is currently registered to, sign in to the [AWS Support Center](#).

Important

You must sign in either by using the root account or by using an IAM user that has been granted IAM permissions in one or more of the following ways:

- The user is assigned the **AdministratorAccess** managed policy.

- The user is assigned the **AmazonRoute53DomainsFullAccess** managed policy.
- The user is assigned the **AmazonRoute53FullAccess** managed policy.
- The user is assigned the **PowerUserAccess** managed policy.
- The user has permission to perform all the following actions: `TransferDomains`, `DisableDomainTransferLock`, and `RetrieveDomainAuthCode`.

If you don't sign in either by using the root account or by using an IAM user that has the required permissions, we can't perform the transfer. This requirement prevents unauthorized users from transferring domains to other AWS accounts.

2. **Note**

Domains can't be transferred within the first 14 days of registration.

Specify the following values. The form automatically fills in the first three values:

Option buttons directly below Create case

Accept the default value of **Account and Billing Support**.

Service

Accept the default value of **Billing**.

Category

Accept the default value of **Domain name registration issue**.

Subject

Specify **Transfer a domain to another AWS account**.

Description

Provide the following information:

- Domain that you want to transfer
- **12-digit account ID** of the AWS account that the domain is currently registered to
- **12-digit account ID** of the AWS account that you want to transfer domain registration to

Contact method

Choose a contact method, **Web** or **Phone**. If you choose **Web**, we'll contact you using the email address that's associated with your AWS account. If you choose **Phone**, enter the applicable values.

3. Choose **Submit**.

Account B has three days to accept the transfer from account A by using the [transfer-domain-to-another-aws-account](#) API. If the transfer isn't accepted in 3 days, the transfer request is cancelled.

Step 2 (Optional): Migrate a hosted zone to a different AWS account

If you're using Route 53 as the DNS service for the domain, Route 53 doesn't transfer the hosted zone when you transfer a domain to a different AWS account. If domain registration is associated with one account and the corresponding hosted zone is associated with another account, neither domain registration nor DNS functionality is affected. The only effect is that you'll need to sign into the Route 53 console using one account to see the domain, and sign in using the other account to see the hosted zone.

If you own the account that you're transferring the domain from and the account that you're transferring the domain to, you can optionally migrate the hosted zone for the domain to a different account, but it's

not required. Route 53 will continue to use the records in the existing hosted zone to route traffic for the domain.

Important

If you don't own both the account that you're transferring the domain from and the account that you're transferring the domain to, you must either migrate the existing hosted zone to the AWS account that you're transferring the domain to, or create a new hosted zone in an AWS account that you own. If you don't own the account that created the hosted zone that routes traffic for the domain, you can't control how traffic is routed.

To migrate the existing hosted zone to the new account, see [Migrating a hosted zone to a different AWS account \(p. 363\)](#).

To create a new hosted zone, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#). This topic is typically used when you're transferring domains from another registrar to Route 53, but the process is the same when you're transferring domains from one AWS account to another.

Transferring a domain from Amazon Route 53 to another registrar

When you transfer a domain from Amazon Route 53 to another registrar, you get some information from Route 53 and provide it to the new registrar. The new registrar will do the rest.

Important

If you're currently using Route 53 as your DNS service provider and you also want to transfer DNS service to another provider, be aware that the following Route 53 features don't have direct parallels with features provided by other DNS service providers. You'll need to work with the new DNS service provider to determine how to achieve comparable functionality:

- Alias records. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).
- Routing policies other than the simple routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).
- Health checks that are associated with records. For more information, see [Configuring DNS failover \(p. 536\)](#).

Most domain registrars enforce requirements on transferring a domain to another registrar. The primary purpose of these requirements is to prevent the owners of fraudulent domains from repeatedly transferring the domains to different registrars. Requirements vary, but the following requirements are typical:

- You must have registered the domain with the current registrar or transferred registration for the domain to the current registrar at least 60 days ago.
- If the registration for a domain name expired and had to be restored, it must have been restored at least 60 days ago.
- The domain cannot have any of the following domain name status codes:
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - clientTransferProhibited

For a current list of domain name status codes and an explanation of what each code means, go to the [ICANN website](#) and search for **epp status codes**. (Search on the ICANN website; web searches sometimes return an old version of the document.)

Note

If you want to transfer your domain to another domain registrar but the AWS account that the domain is registered with is closed, suspended, or terminated, you can contact AWS Support for help. Domains cannot be transferred within the first 14 days of registration. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

To transfer a domain from Route 53 to another registrar

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain that you want to transfer to another registrar.
4. On the **Registered domains > domain name** page, check the value of **Domain name status code**. If it is one of the following values, you can't currently transfer the domain:
 - pendingDelete
 - pendingTransfer
 - redemptionPeriod
 - clientTransferProhibited
 - serverTransferProhibited

For a current list of domain name status codes and an explanation of what each code means, go to the [ICANN website](#) and search for **epp status codes**. (Search on the ICANN website; web searches sometimes return an old version of the document.)

If the value of **Domain name status code** is **serverTransferProhibited**, you can contact AWS Support for free to learn what you must do so you can transfer the domain. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

5. If the value of **Transfer lock** is **Enabled**, choose **Disable**.
6. Choose **Save**.
7. *All domains except .co.za, .es, .jp, .ru, .uk, .co.uk, .me.uk, and .org.uk domains – On the **Registered Domains > domain name** page, at **Authorization Code**, choose **Get code** and make note of the authorization code. You'll provide this value to your registrar later in this procedure.*

.co.za, .es, .jp, .ru, .uk, .co.uk, .me.uk, and .org.uk domains – Do the following:

.co.za domains

You don't need to get an authorization code to transfer a .co.za domain to another registrar.

.es domains

You don't need to get an authorization code to transfer a .es domain to another registrar.

.jp domains

You don't need to get an authorization code to initiate the transfer at your new registrar, but you'll need one to confirm the transfer.

.ru domains

Get the authorization code from the registry for .ru domains at <https://www.nic.ru/en/auth/recovery/>:

- a. Choose the option to recover credentials by domain name.
- b. Enter your domain name, and choose **Continue**.

- c. Follow the on-screen prompts to get access to the RU-CENTER admin page.

- d. In the **Manage your account** section, choose **Domain transfer**.

- e. Confirm the transfer with REGRU-RU.

.uk, .co.uk, .me.uk, and .org.uk domains

Change the IPS tag to the value for the new registrar:

- a. Go to the [Find a Registrar](#) page on the Nominet website, and find the IPS tag for the new registrar. (Nominet is the registry for .uk, .co.uk, .me.uk, and .org.uk domains.)
- b. On the **Registered Domains > domain name** page, at **IPS Tag**, choose **Change IPS Tag**, and specify the value that you got in step 7a.
- c. Choose **Update**.

8. If you're not currently using Route 53 as the DNS service provider for your domain, skip to step 10.

If you are currently using Route 53 as the DNS service provider for the domain, perform the following steps:

- a. Choose **Hosted Zones**.
- b. Choose the name of the hosted zone for your domain. The domain and the hosted zone have the same name.
- c. *If you want to continue using Route 53 as the DNS service provider for the domain:* Get the names of the four name servers that Route 53 assigned to your hosted zone. For more information, see [Getting the name servers for a public hosted zone \(p. 341\)](#).

If you do not want to continue using Route 53 as the DNS service provider for the domain: Make note of the settings for all of your records except the NS and SOA records. For Route 53-specific features such as alias records, you'll need to work with your new DNS service provider to determine how to achieve comparable functionality.

9. If you're transferring DNS service to another provider, use the methods that are provided by the new DNS service to perform the following tasks:

- Create a hosted zone
- Create records that reproduce the functionality of your Route 53 records
- Get the name servers that the new DNS service assigned to your hosted zone

10. Use the process that is provided by the new registrar to request a transfer of the domain.

All domains except .co.za, .es, .jp, .uk, .co.uk, .me.uk, and .org.uk domains – You'll be prompted to enter the authorization code that you got from the Route 53 console in step 7 of this procedure.

11. If you still want to use Route 53 as your DNS service provider, use the process that is provided by the new registrar to specify the names of the Route 53 name servers that you got in step 8. If you want to use another DNS service provider, specify the names of the name servers that the new provider gave you when you created a new hosted zone in step 9.

12. Respond to the confirmation email:

All domains except .jp domains

Route 53 sends a confirmation email to the email address for the registrant contact for the domain:

- If you don't respond to the email, the transfer happens automatically on the specified date.
- If you want the transfer to happen sooner or you want to cancel the transfer, choose the link in the email to go to the Route 53 website, and choose the applicable option.

.jp domains

Route 53 sends a confirmation email to the email address for the registrant contact for the domain from address *noreply@domainnameverification.net* with a link to confirm the transfer:

- If you don't respond to the email, the transfer is canceled on the specified date.

- If you want the transfer to happen sooner or you want to cancel the transfer, choose the link in the email to go to the Route 53 website, and choose the applicable option. You will be required to provide the domain authorization code that you obtained in step 7.

In addition you might receive an email from WIXI.jp. You can ignore this email.

13. If the registrar that you're transferring the domain to reports that the transfer failed, contact that registrar for more information. When you transfer a domain to another registrar, all status updates go to the new registrar, so Route 53 has no information about why a transfer failed.

If the new registrar reports that the transfer failed because the authorization code that you got from Route 53 isn't valid, open a case with AWS Support. (You don't need a support contract, and there's no fee.) For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

14. If you transferred DNS service to another DNS service provider, you can delete the records in the hosted zone and delete the hosted zone after DNS resolvers stop responding to DNS queries with the names of Route 53 name servers. This typically takes two days, the amount of time that DNS resolvers commonly cache the names of name servers for a domain.

Important

If you delete the hosted zone while DNS resolvers are still responding to DNS queries with the names of Route 53 name servers, your domain will become unavailable on the internet.

After you delete the hosted zone, Route 53 will stop billing you the monthly charge for a hosted zone. For more information, see the following documentation:

- [Deleting records \(p. 440\)](#)
- [Deleting a public hosted zone \(p. 345\)](#)
- [Route 53 Pricing](#)

Resending authorization and confirmation emails

For several operations related to domain registration, ICANN requires that we get authorization from the registrant contact for the domain or confirmation that the email address for the registrant contact is valid. To get authorization or confirmation, we send an email that contains a link. You have between 3 and 15 days to click the link, depending on the operation and the top-level domain. After that time, the link stops working.

If you don't click the link in the email in the allotted amount of time, ICANN generally requires that we suspend the domain or cancel the operation, depending on what you were trying to do:

Register a domain

We suspend the domain, so that it's not accessible on the internet. To resend the confirmation email, see [To resend the confirmation email for a domain registration \(p. 87\)](#).

Geographic TLDs only – Transfer a domain to Amazon Route 53

If you're transferring a domain that has a [geographic TLD](#), we cancel the transfer. To resend the authorization email, see [To resend the authorization email for a domain transfer \(p. 88\)](#).

Note

Authorization isn't required for domains that have a [generic TLD](#), such as .com, .net, or .org.

Change the name or email address of the registrant contact for the domain (the owner)

We cancel the change. To resend the authorization email, see [To resend the authorization email to update the registrant contact or delete a domain \(p. 89\)](#).

Delete a domain

We cancel the deletion request. To resend the authorization email, see [To resend the authorization email to update the registrant contact or delete a domain \(p. 89\)](#).

Geographic TLDs only – Transfer a domain from Route 53 to another registrar

If you're transferring a domain that has a [geographic TLD](#), the new registrar cancels the transfer.

Note

Authorization isn't required for domains that have a [generic TLD](#), such as .com, .net, or .org.

Topics

- [Updating your email address \(p. 87\)](#)
- [Resending emails \(p. 87\)](#)

Updating your email address

We always send confirmation and authorization emails to the email address for the registrant contact for a domain. For some TLDs, we're required to send email to the old and new email addresses for the registrant contact in the following cases:

- You're changing the email address for a domain that is already registered with Amazon Route 53
- You're changing the email address for a domain that you're transferring to Route 53

Resending emails

Use the applicable procedure to resend confirmation or authorization emails.

- [To resend the confirmation email for a domain registration \(p. 87\)](#)
- [To resend the authorization email for a domain transfer \(p. 88\)](#)
- [To resend the authorization email to update the registrant contact or delete a domain \(p. 89\)](#)

To resend the confirmation email for a domain registration

1. Check the email address for the registrant contact and, if necessary, update it. For more information, see [Updating contact information and ownership for a domain \(p. 52\)](#).
2. Check the spam folder in your email application for an email from one of the following email addresses.

If too much time has passed, the link won't work any longer, but you'll know where to look for the confirmation email when we send you another one.

TLDs	Email address that the approval or confirmation email comes from
.fr	nic@nic.fr
All others	One of the following email addresses: <ul style="list-style-type: none">• noreply@registrar.amazon.com• noreply@domainnameverification.net

3. Use the Amazon Route 53 console to resend the confirmation email:

- a. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
- b. In the navigation pane, choose **Registered domains**.
- c. Choose the name of the domain that you want to resend the email for.
- d. In the warning box with the heading "Your domain might be suspended," choose **Send email again**.

Note

If there's no warning box, you already confirmed that the email address for the registrant contact is valid.

4. If you encounter issues while resending the confirmation email, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

To resend the authorization email for a domain transfer

This method doesn't work for .jp domain transfer out requests.

1. Use the method provided by the current domain registrar to confirm that privacy protection for the domain is disabled. If not, disable it.

We send the authorization email to the email address that the current registrar saved in the WHOIS database. When privacy protection is enabled, that email address typically is obfuscated. The current registrar might not forward to your actual email address the email that Amazon Route 53 sends to the email address in the WHOIS database.

Note

If the current registrar for the domain won't let you turn off privacy protection, we can still transfer the domain if you specified a valid authorization code in [Step 5: Request the transfer \(p. 71\)](#).

2. Check the email address for the registrant contact and, if necessary, update it. Use the method provided by the current registrar for the domain.
3. Check the spam folder in your email application for an email from one of the following email addresses.

If too much time has passed, the link won't work any longer, but you'll know where to look for the authorization email when we send you another one.

TLDs	Email address that the approval or confirmation email comes from
.com.au and .net.au	no-reply@ispapi.net The email contains a link to https://approve.domainadmin.com .
.fr	nic@nic.fr
All others	One of the following email addresses: <ul style="list-style-type: none">• noreply@registrar.amazon.com• noreply@domainnameverification.net

4. If the transfer is no longer in process (if we already canceled it because too much time has passed), request the transfer again, and we'll send you another authorization email.

Note

For the first 15 days after you request a transfer, you can determine the status of the transfer by checking the **Notifications** table on the **Dashboard** page in the Route 53

console. After 15 days, use the AWS CLI to get the status. For more information, see [route53domains](#) in the *AWS CLI Command Reference*.

If the transfer is still in progress, perform the following steps to resend the authorization email.

- a. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
- b. In the **Notifications** table, find the domain that you want to transfer.
- c. In the **Status** column for that domain, choose **Resend email**.
5. If you encounter issues while resending the authorization email for a domain transfer, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

To resend the authorization email to update the registrant contact or delete a domain

1. Check the email address for the registrant contact and, if necessary, update it. For more information, see [Updating contact information and ownership for a domain \(p. 52\)](#).
2. Check the spam folder in your email application for an email from one of the following email addresses.

If too much time has passed, the link won't work any longer, but you'll know where to look for the authorization email when we send you another one.

TLDs	Email address that the authorization email comes from
.fr	nic@nic.fr
All others	One of the following email addresses: <ul style="list-style-type: none">• noreply@registrar.amazon.com• noreply@domainnameverification.net

3. Cancel the change or deletion. You have two options:
 - You can wait for the 3 to 15 day waiting period to pass, after which we automatically cancel the requested operation.
 - Alternatively, you can contact AWS Support and ask them to cancel the operation.
4. After the change or deletion is canceled, you can change the contact information or delete the domain again, and we'll send you another authorization email.
5. If you encounter issues while resending the authorization email, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Configuring DNSSEC for a domain

Attackers sometimes hijack traffic to internet endpoints such as web servers by intercepting DNS queries and returning their own IP addresses to DNS resolvers in place of the actual IP addresses for those endpoints. Users are then routed to the IP addresses provided by the attackers in the spoofed response, for example, to fake websites.

You can protect your domain from this type of attack, known as DNS spoofing or a man-in-the-middle attack, by configuring Domain Name System Security Extensions (DNSSEC), a protocol for securing DNS traffic.

Important

Amazon Route 53 supports DNSSEC signing as well as DNSSEC for domain registration. If you want to configure DNSSEC signing for a domain that's registered with Route 53, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

Topics

- [Overview of how DNSSEC protects your domain \(p. 90\)](#)
- [Prerequisites and maximums for configuring DNSSEC for a domain \(p. 91\)](#)
- [Adding public keys for a domain \(p. 91\)](#)
- [Deleting public keys for a domain \(p. 92\)](#)

Overview of how DNSSEC protects your domain

When you configure DNSSEC for your domain, a DNS resolver establishes a chain of trust for responses from intermediate resolvers. The chain of trust begins with the TLD registry for the domain (your domain's parent zone) and ends with the authoritative name servers at your DNS service provider. Not all DNS resolvers support DNSSEC. Resolvers that don't support DNSSEC don't perform any signature or authenticity validation.

Here's how you configure DNSSEC for domains registered with Amazon Route 53 to protect your internet hosts from DNS spoofing, simplified for clarity:

1. Use the method provided by your DNS service provider to *sign* the records in your hosted zone with the *private key* in an asymmetric key pair.

Important

Route 53 supports DNSSEC signing as well as DNSSEC for domain registration. To learn more, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

2. Provide the *public key* from the key pair to your domain registrar, and specify the algorithm that was used to generate the key pair. The domain registrar forwards the public key and the algorithm to the registry for the top-level domain (TLD).

For information about how to perform this step for domains that you registered with Route 53, see [Adding public keys for a domain \(p. 91\)](#).

After you configure DNSSEC, here's how it protects your domain from DNS spoofing:

1. Submit a DNS query, for example, by browsing to a website or by sending an email message.
2. The request is routed to a DNS resolver. Resolvers are responsible for returning the appropriate value to clients based on the request, for example, the IP address for the host that is running a web server or an email server.
3. If the IP address is cached on the DNS resolver (because someone else has already submitted the same DNS query, and the resolver already got the value), the resolver returns the IP address to the client that submitted the request. The client then uses the IP address to access the host.

If the IP address isn't cached on the DNS resolver, the resolver sends a request to the parent zone for your domain, at the TLD registry, which returns two values:

- The Delegation Signer (DS) record, which is a public key that corresponds with the private key that was used to sign the record.
 - The IP addresses of the authoritative name servers for your domain.
4. The DNS resolver sends the original request to another DNS resolver. If that resolver doesn't have the IP address, it repeats the process until a resolver sends the request to a name server at your DNS service provider. The name server returns two values:
 - The record for the domain, such as example.com. Typically this contains the IP address of a host.

- The signature for the record, which you created when you configured DNSSEC.
5. The DNS resolver uses the public key that you provided to the domain registrar (and the registrar forwarded to the TLD registry) to do two things:
 - Establish a chain of trust.
 - Verify that the signed response from the DNS service provider is legitimate and hasn't been replaced with a bad response from an attacker.
 6. If the response is authentic, the resolver returns the value to the client that submitted the request.

If the response can't be verified, the resolver returns an error to the user.

If the TLD registry for the domain doesn't have the public key for the domain, the resolver responds to the DNS query by using the response that it got from the DNS service provider.

Prerequisites and maximums for configuring DNSSEC for a domain

To configure DNSSEC for a domain, your domain and DNS service provider must meet the following prerequisites:

- The registry for the TLD must support DNSSEC. To determine whether the registry for your TLD supports DNSSEC, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).
- The DNS service provider for the domain must support DNSSEC.

Important

Route 53 supports DNSSEC signing as well as DNSSEC for domain registration. To learn more, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

- You must configure DNSSEC with the DNS service provider for your domain before you add public keys for the domain to Route 53.
- The number of public keys that you can add to a domain depends on the TLD for the domain:
 - **.com and .net domains** – up to thirteen keys
 - **All other domains** – up to four keys

Adding public keys for a domain

When you're rotating keys or you're enabling DNSSEC for a domain, perform the following procedure after you configure DNSSEC with the DNS service provider for the domain.

To add public keys for a domain

1. If you haven't already configured DNSSEC with your DNS service provider, use the method provided by your service provider to configure DNSSEC.
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Registered domains**.
4. Choose the name of the domain that you want to add keys for.
5. At the **DNSSEC status** field, choose **Manage keys**.
6. Specify the following values:

Key type

Choose whether you want to upload a key-signing key (KSK) or a zone-signing key (ZSK).

Algorithm

Choose the algorithm that you used to sign the records for the hosted zone.

Public key

Specify the public key from the asymmetric key pair that you used to configure DNSSEC with your DNS service provider.

Note the following:

- Specify the public key, not the digest.
- You must specify the key in base64 format.

7. Choose **Add**.

Note

You can only add one public key at a time. If you need to add more keys, wait until you receive a confirmation email from Route 53.

8. When Route 53 receives a response from the registry, we send an email to the registrant contact for the domain. The email either confirms that the public key has been added to the domain at the registry or explains why the key couldn't be added.

Deleting public keys for a domain

When you're rotating keys or you're disabling DNSSEC for the domain, delete public keys using the following procedure before you disable DNSSEC with your DNS service provider. Note the following:

- If you're rotating public keys, we recommend that you wait for up to three days after you add the new public keys to delete the old public keys.
- If you're disabling DNSSEC, delete public keys for the domain first. We recommend that you wait for up to three days before you disable DNSSEC with the DNS service for the domain.

Important

If DNSSEC is enabled for the domain and you disable DNSSEC with the DNS service, DNS resolvers that support DNSSEC will return a `SERVFAIL` error to clients, and the clients won't be able to access the endpoints that are associated with the domain.

To delete public keys for a domain

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered domains**.
3. Choose the name of the domain that you want to delete keys from.
4. At the **DNSSEC status** field, choose **Manage keys**.
5. Find the key that you want to delete, and choose **Delete**.

Note

You can only delete one public key at a time. If you need to delete more keys, wait until you receive a confirmation email from Amazon Route 53.

6. When Route 53 receives a response from the registry, we send an email to the registrant contact for the domain. The email either confirms that the public key has been deleted from the domain at the registry or explains why the key couldn't be deleted.

Viewing information about domains that are registered with Amazon Registrar

You can view information about .com, .net, and .org domains that were registered using Route 53 and for which Amazon Registrar is the registrar. This information includes details such as when the domain was originally registered and contact information for the domain owner and for the technical and administrative contacts.

Note the following:

Emailing domain contacts when privacy protection is enabled

If privacy protection is enabled for the domain, contact information for the registrant, technical, and administrative contacts is replaced with contact information for the Amazon Registrar privacy service. For example, if the example.com domain is registered with Amazon Registrar and if privacy protection is enabled, the value of **Registrant Email** in the response to a WHOIS query would be similar to owner123@example.com.whoisprivacyservice.org.

To contact one or more domain contacts when privacy protection is enabled, send an email to the corresponding email addresses. We automatically forward your email to the applicable contact.

Reporting abuse

To report any illegal activity or violation of the [Acceptable Use Policy](#), including inappropriate content, phishing, malware, or spam, send an email to abuse@amazon.com.

To view information about domains that are registered with Amazon Registrar

1. In a web browser, go to one of the following websites. Both websites display the same information, they just use different protocols and display the information in different formats:
 - **WHOIS:** <https://registrar.amazon.com/whois>
 - **RDAP:** <https://registrar.amazon.com/rdap>
2. Enter the name of the domain that you want to view information about, and choose **Search**.

Deleting a domain name registration

For most top-level domains (TLDs), you can delete the registration if you no longer want it. If the registry allows you to delete the registration, perform the procedure in this topic.

Note the following:

The registration fee is not refundable

If you delete a domain name registration before the registration is scheduled to expire, AWS does not refund the registration fee.

TLDs that allow you to delete a domain registration

To determine whether you can delete the registration for your domain, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#). If the section for your TLD doesn't include a "Deletion of domain registration" subsection, you can delete the domain.

What if you can't delete a domain registration?

If the registry for your domain doesn't allow you to delete a domain name registration, you must wait for the domain to expire. To ensure that the domain isn't automatically renewed, disable

automatic renewal for the domain. When the **Expires on** date passes, Route 53 automatically deletes the registration for the domain. For information about how to change the automatic renewal setting, see [Enabling or disabling automatic renewal for a domain \(p. 59\)](#).

Delay before a domain is deleted and available to register again

Almost all registries prevent anyone from immediately registering a domain that has just expired. The typical delay is one to three months, depending on the TLD. For more information, see the "Deadlines for renewing and restoring domains" section for your TLD in [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

Important

Don't delete a domain and expect to reregister it if you just want to transfer the domain between AWS accounts or transfer the domain to another registrar. See the applicable documentation instead:

- [Transferring a domain to a different AWS account \(p. 81\)](#)
- [Transferring a domain from Amazon Route 53 to another registrar \(p. 83\)](#)

To delete a domain name registration

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 2. In the navigation pane, choose **Registered Domains**.
 3. Choose the name of your domain.
- If you want to delete a .com.uk, .me.uk, .org.uk, or .uk domain, see [To delete .com.uk, .me.uk, .org.uk, and .uk domain name registrations \(p. 95\)](#).
4. Choose **Delete Domain**.
 5. If the registry for your TLD allows deleting a domain name registration, choose **Delete Domain**.

We send an email to the registrant for the domain to verify that the registrant wants to delete the domain. (This is an ICANN requirement.) The email comes from one of the following email addresses:

- noreply@registrar.amazon.com – for TLDs registered by Amazon Registrar.
- noreply@domainnameverification.net – for TLDs registered by our registrar associate, Gandi.

To determine who the registrar is for your TLD, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

6. When you receive the verification email, choose the link in the email, and either approve or reject the request to delete the domain.

Important

The registrant contact must follow the instructions in the email, or we must cancel the deletion request after five days as required by ICANN.

You'll receive another email when your domain has been deleted. To determine the current status of your request, see [Viewing the status of a domain registration \(p. 52\)](#).

7. Delete the records in the hosted zone for the deleted domain, and then delete the hosted zone. After you delete the hosted zone, Route 53 stops billing you the monthly charge for a hosted zone. For more information, see the following documentation:
 - [Deleting records \(p. 440\)](#)
 - [Deleting a public hosted zone \(p. 345\)](#)
 - [Route 53 Pricing](#)
8. If you encounter issues while deleting a domain name registration, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

To delete .com.uk, .me.uk, .org.uk, and .uk domain name registrations

If you want to delete a .com.uk, .me.uk, .org.uk, or .uk domain, you create an account with Nominet, the registry for .uk domains. For more information, see "Cancelling your domain name" on the Nominet website, <https://www.nominet.uk/domain-support/>.

Important

If you delete (cancel) a .uk domain name, it's deleted by the end of the day and becomes available for anyone to register. If you just want to transfer the domain, do not delete it.

Here's an overview of the process:

1. On the Nominet website, follow the instructions for logging in for the first time. See <https://secure.nominet.org.uk/auth/login.html>. Nominet sends you an email with instructions for creating a password.
2. Follow the instructions in the email that you receive from Nominet.
3. Log in to the Nominet website, and follow the instructions for canceling (deleting) a domain name.

Contacting AWS Support about domain registration issues

AWS provides a Basic support plan, free of charge, for all AWS customers. The plan includes assistance for the following issues related to domain registration:

- Transferring domains to or from Amazon Route 53
- Transferring domains between AWS accounts
- Increasing quotas on Route 53 entities, such as the number of domains that you can register (See [Quotas \(p. 671\)](#).)
- Changing the owner of a domain
- Changing contact information for the owner of a domain
- Resending confirmation and authorization emails
- Renewing domains
- Restoring expired domains
- Getting information about Route 53 billing
- Providing proof of identity for .uk domains
- Deleting domains or disabling automatic renewal after you close your AWS account

To contact AWS Support about these and other issues related to domain registration, perform the applicable procedure.

Topics

- [Contacting AWS Support when you can sign in to your AWS account \(p. 95\)](#)
- [Contacting AWS Support when you can't sign in to your AWS account \(p. 96\)](#)

Contacting AWS Support when you can sign in to your AWS account

To contact AWS Support when you're able to sign in to your AWS account, perform the following procedure:

1. Using the AWS account that the domain is currently registered to, sign in to the [AWS Support Center](#).

Important

You must sign in by using the root account that the domain is currently registered to. This requirement prevents unauthorized users from hijacking your account.

2. Specify the following values:

Regarding

Accept the default value of **Account and Billing Support Service**.

Accept the default value of **Billing Category**.

Accept the default value of **Domain name registration issue**.

Severity

Choose the applicable severity.

Subject

Enter a brief summary of the issue.

Description

Describe the issue that you're having in more detail, and attach any relevant documents or screenshots.

Contact method

Choose a contact method, **Web** or **Phone**. If you choose **Web**, we'll contact you using the email address that's associated with your AWS account. If you choose **Phone**, enter the applicable values.

3. Choose **Submit**.

Contacting AWS Support when you can't sign in to your AWS account

To contact AWS Support when you can't sign in to your AWS account, perform the following procedure:

1. Go to the [I'm an AWS customer and I'm looking for billing or account support](#) page.
2. Fill out the form.
3. Choose **Submit**.

Downloading a domain billing report

If your AWS bill is charged to a credit card, you receive a separate invoice for each domain transaction. These invoices don't include the domain name. If you manage multiple domains and you want to view charges by domain for a specified time period, you can download a domain billing report. This report includes all charges that apply to domain registration, including the following:

- Registering a domain
- Renewing registration for a domain

- Transferring a domain to Amazon Route 53
- Changing the owner of a domain (for some TLDs, this operation is free)

Note

If you use invoiced payments, any Route 53 domain registration transactions appear in your monthly AWS invoice. The invoice includes the domain name and operation that each charge applies to.

When you run the report using the console, you can choose the following options:

- **Last 12 months:** The report includes charges from one year before you ran the report until the current day. For example, if you run the report on June 3rd, it includes charges from June 3rd the previous year until the current day.
- **Individual months in the last year:** The report includes charges for the specified month.

If you run the report programmatically, you can get charges for any date range, starting with July 31, 2014. That's the date that Route 53 started to support domain registration. For example, see [view-billing](#) in the *AWS CLI Command Reference*.

The billing report, in CSV format, includes the following values:

- The AWS invoice ID that the charge appears on.
- The operation (REGISTER_DOMAIN, RENEW_DOMAIN, TRANSFER_IN_DOMAIN, or CHANGE_DOMAIN_OWNER).
- The name of the domain.
- The charge for the operation in US dollars.
- The date and time in ISO 8601 format, for example, 2016-03-03T19:20:25.177Z. For more information about ISO 8601 format, see the Wikipedia article [ISO 8601](#).

To download a domain billing report

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Registered Domains**.
3. Choose **Domain billing report**.
4. Choose the date range for the report, and then choose **Download domain report**.
5. Follow the prompts to open the report or to save it.
6. If you encounter issues while downloading a domain billing report, you can contact AWS Support for free. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Domains that you can register with Amazon Route 53

The following lists of generic and geographic top-level domains show the top-level domains (TLDs) that you can use to register domains with Amazon Route 53. We continue to add support for more TLDs, and we decide which TLDs to add based in part on customer feedback. To suggest a TLD that you'd like us to add, enter a comment on the [Amazon Route 53 Domain Registration forum](#).

Registering domains with Route 53

You can register a domain with Route 53 if the TLD is included on the following lists. If the TLD isn't included, you can't register the domain with Route 53.

Transferring domains to Route 53

You can transfer a domain to Route 53 if the TLD is included on the following lists. If the TLD isn't included, you can't transfer the domain to Route 53.

For most TLDs, you need to get an authorization code from the current registrar to transfer a domain. To determine whether you need an authorization code, see the "Authorization code required for transfer to Route 53" section for your TLD.

Pricing for domain registration and transfers

For information about the cost to register domains or transfer them to Route 53, see [Amazon Route 53 Pricing for Domain Registration](#).

Using Route 53 as your DNS service

You can use Route 53 as the DNS service for any domain, even if the TLD for the domain isn't included on the following lists. For more information about Route 53 as a DNS service, see [How internet traffic is routed to your website or web application \(p. 2\)](#). For information about how to transfer DNS service for your domain to Route 53, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Internationalized domain names

Not all TLDs support internationalized domain names (IDNs), meaning domain names that include characters other than ASCII characters a-z, 0-9, and - (hyphen). The listing for each TLD indicates whether that TLD supports IDNs. For more information about internationalized domain names, see [DNS domain name format \(p. 38\)](#).

Registering geographic domains with TLDs

The rules for registration of geographic TLDs vary by country. Some countries are unrestricted, meaning that anyone in the world can register, while others have certain restrictions, such as residency. The listing for each geographic TLD indicates any restrictions.

Index to supported top-level domains

Topics

- [Generic top-level domains \(p. 98\)](#)
- [Geographic top-level domains \(p. 100\)](#)

Generic top-level domains

[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 \(p. 103\)](#), [.academy \(p. 103\)](#), [.accountants \(p. 104\)](#), [.adult \(p. 104\)](#), [.agency \(p. 105\)](#),
[.apartments \(p. 106\)](#), [.associates \(p. 106\)](#), [.auction \(p. 107\)](#), [.audio \(p. 108\)](#)

B

[.band \(p. 108\)](#), [.bargains \(p. 109\)](#), [.bike \(p. 110\)](#), [.bingo \(p. 110\)](#), [.biz \(p. 111\)](#),
[.black \(p. 112\)](#), [.blue \(p. 112\)](#), [.boutique \(p. 113\)](#), [.builders \(p. 114\)](#), [.business \(p. 114\)](#),
[.buzz \(p. 115\)](#)

C

.cab (p. 116), .cafe (p. 116), .camera (p. 117), .camp (p. 118), .capital (p. 118),
.cards (p. 119), .care (p. 120), .careers (p. 120), .cash (p. 121), .casino (p. 122),
.catering (p. 122), .cc (p. 123), .center (p. 123), .ceo (p. 124), .chat (p. 124), .cheap (p. 125),
.church (p. 126), .city (p. 126), .claims (p. 127), .cleaning (p. 128), .click (p. 128),
.clinic (p. 129), .clothing (p. 130), .cloud (p. 130), .club (p. 131), .coach (p. 132),
.codes (p. 132), .coffee (p. 133), .college (p. 134), .com (p. 134), .community (p. 135),
.company (p. 136), .computer (p. 136), .condos (p. 137), .construction (p. 138),
.consulting (p. 138), .contractors (p. 139), .cool (p. 140), .coupons (p. 140), .credit (p. 141),
.creditcard (p. 142), .cruises (p. 142)

D

.dance (p. 143), .dating (p. 144), .deals (p. 144), .delivery (p. 145), .democrat (p. 146),
.dental (p. 146), .diamonds (p. 147), .diet (p. 148), .digital (p. 148), .direct (p. 149),
.directory (p. 150), .discount (p. 150), .dog (p. 151), .domains (p. 152)

E

.education (p. 152), .email (p. 153), .energy (p. 154), .engineering (p. 154),
.enterprises (p. 155), .equipment (p. 156), .estate (p. 156), .events (p. 157),
.exchange (p. 158), .expert (p. 158), .exposed (p. 159), .express (p. 160)

F

.fail (p. 160), .farm (p. 161), .finance (p. 162), .financial (p. 162), .fish (p. 163),
.fitness (p. 164), .flights (p. 164), .florist (p. 165), .flowers (p. 166), .fm (p. 166),
.football (p. 166), .forsale (p. 167), .foundation (p. 168), .fund (p. 168), .furniture (p. 169),
.futbol (p. 170), .fyi (p. 170)

G

.gallery (p. 171), .gift (p. 172), .gifts (p. 172), .glass (p. 173), .global (p. 174), .gold (p. 174),
.golf (p. 175), .graphics (p. 176), .gratis (p. 176), .green (p. 177), .gripe (p. 178),
.guide (p. 178), .guitars (p. 179), .guru (p. 180)

H

.haus (p. 180), .healthcare (p. 181), .help (p. 182), .hiv (p. 182), .hockey (p. 183),
.holdings (p. 184), .holiday (p. 184), .host (p. 185), .hosting (p. 186), .house (p. 186)

I

.im (p. 187), .immo (p. 187), .immobilien (p. 188), .industries (p. 188), .info (p. 189),
.ink (p. 190), .institute (p. 190), .insure (p. 191), .international (p. 192), .investments (p. 192),
.io (p. 193), .irish (p. 193)

J

.jewelry (p. 194), .juegos (p. 194)

K

.kaufen (p. 195), .kim (p. 196), .kitchen (p. 196), .kiwi (p. 197)

L

.land (p. 198), .lease (p. 198), .legal (p. 199), .lgbt (p. 200), .life (p. 200), .lighting (p. 201),
.limited (p. 202), .limo (p. 202), .link (p. 203), .live (p. 204), .loan (p. 204), .loans (p. 205),
.lol (p. 206)

M

.maison (p. 206), .management (p. 207), .marketing (p. 208), .mba (p. 208), .media (p. 209),
.memorial (p. 210), .mobi (p. 210), .moda (p. 211), .money (p. 212), .mortgage (p. 212),
.movie (p. 213)

N

[.name](#) (p. 214), [.net](#) (p. 214), [.network](#) (p. 215), [.news](#) (p. 216), [.ninja](#) (p. 216)

O

[.onl](#) (p. 217), [.online](#) (p. 218), [.org](#) (p. 218)

P

[.partners](#) (p. 219), [.parts](#) (p. 220), [.photo](#) (p. 220), [.photography](#) (p. 221), [.photos](#) (p. 222),
[.pics](#) (p. 222), [.pictures](#) (p. 223), [.pink](#) (p. 224), [.pizza](#) (p. 224), [.place](#) (p. 225),
[.plumbing](#) (p. 226), [.plus](#) (p. 226), [.poker](#) (p. 227), [.porn](#) (p. 228), [.pro](#) (p. 228),
[.productions](#) (p. 229), [.properties](#) (p. 230), [.property](#) (p. 230), [.pub](#) (p. 231)

Q

[.qpon](#) (p. 232)

R

[.recipes](#) (p. 232), [.red](#) (p. 233), [.reise](#) (p. 234), [.reisen](#) (p. 234), [.rentals](#) (p. 235),
[.repair](#) (p. 236), [.report](#) (p. 236), [.republican](#) (p. 237), [.restaurant](#) (p. 238), [.reviews](#) (p. 238),
[.rip](#) (p. 239), [.rocks](#) (p. 240), [.run](#) (p. 240)

S

[.sale](#) (p. 241), [.sarl](#) (p. 242), [.school](#) (p. 242), [.schule](#) (p. 243), [.services](#) (p. 244), [.sex](#) (p. 244),
[.sexy](#) (p. 245), [.shiksha](#) (p. 246), [.shoes](#) (p. 246), [.show](#) (p. 247), [.singles](#) (p. 248),
[.soccer](#) (p. 248), [.social](#) (p. 249), [.solar](#) (p. 250), [.solutions](#) (p. 250), [.studio](#) (p. 251),
[.style](#) (p. 252), [.sucks](#) (p. 252), [.supplies](#) (p. 253), [.supply](#) (p. 254), [.support](#) (p. 254),
[.surgery](#) (p. 255), [.systems](#) (p. 256)

T

[.tattoo](#) (p. 256), [.tax](#) (p. 257), [.taxi](#) (p. 258), [.team](#) (p. 258), [.technology](#) (p. 259),
[.tennis](#) (p. 260), [.theater](#) (p. 260), [.tienda](#) (p. 261), [.tips](#) (p. 262), [.tires](#) (p. 262),
[.today](#) (p. 263), [.tools](#) (p. 264), [.tours](#) (p. 264), [.town](#) (p. 265), [.toys](#) (p. 266), [.trade](#) (p. 266),
[.training](#) (p. 267), [.tv](#) (p. 268)

U

[.university](#) (p. 268), [.uno](#) (p. 269)

V

[.vacations](#) (p. 270), [.vegas](#) (p. 270), [.ventures](#) (p. 271), [.vg](#) (p. 272), [.viajes](#) (p. 272),
[.video](#) (p. 272), [.villas](#) (p. 273), [.vision](#) (p. 274), [.voyage](#) (p. 274)

WXYZ

[.watch](#) (p. 275), [.website](#) (p. 276), [.wiki](#) (p. 276), [.works](#) (p. 277), [.world](#) (p. 278),
[.wtf](#) (p. 278), [.xyz](#) (p. 279), [.zone](#) (p. 280)

Geographic top-level domains

Africa

[.ac](#) (Ascension Island) (p. 281), [.co.za](#) (South Africa) (p. 282), [.sh](#) (Saint Helena) (p. 283)

Americas

[.ca](#) (Canada) (p. 284), [.cl](#) (Chile) (p. 285), [.co](#) (Colombia) (p. 286), [.com.ar](#) (Argentina) (p. 286),
[.com.br](#) (Brazil) (p. 287), [.com.mx](#) (Mexico) (p. 288), [.mx](#) (Mexico) (p. 288), [.us](#) (United States) (p. 289), [.vc](#) (Saint Vincent and the Grenadines) (p. 290), [.vg](#) (British Virgin Islands) (p. 290)

Asia/Oceania

.au (Australia) (p. 291), .cc (Cocos (Keeling) Islands) (p. 294), .co.nz (New Zealand) (p. 295), .com.au (Australia) (p. 295), .com.sg (Republic of Singapore) (p. 297), .fm (Federated States of Micronesia) (p. 298), .in (India) (p. 298), .jp (Japan) (p. 299), .io (British Indian Ocean Territory) (p. 300), .net.au (Australia) (p. 301), .net.nz (New Zealand) (p. 302), .org.nz (New Zealand) (p. 303), .qa (Qatar) (p. 304), .ru (Russian Federation) (p. 305), .sg (Republic of Singapore) (p. 306)

Europe

.be (Belgium) (p. 307), .berlin (city of Berlin in Germany) (p. 307), .ch (Switzerland) (p. 308), .co.uk (United Kingdom) (p. 309), .cz (Czech Republic) (p. 310), .de (Germany) (p. 310), .es (Spain) (p. 311), .eu (European Union) (p. 312), .fi (Finland) (p. 313), .fr (France) (p. 314), .gg (Guernsey) (p. 315), .im (Isle of Man) (p. 316), .it (Italy) (p. 316), .me (Montenegro) (p. 317), .me.uk (United Kingdom) (p. 318), .nl (the Netherlands) (p. 319), .org.uk (United Kingdom) (p. 320), .ruhr (Ruhr region, western part of Germany) (p. 321), .se (Sweden) (p. 321), .uk (United Kingdom) (p. 322), .wien (city of Vienna in Austria) (p. 323)

Generic top-level domains

Generic top-level domains (gTLDs) are global extensions that are used and recognized around the world, such as .com, .net, and .org. They also include specialty domains such as .bike, .condos, and .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 (p. 103), .academy (p. 103), .accountants (p. 104), .adult (p. 104), .agency (p. 105), .apartments (p. 106), .associates (p. 106), .auction (p. 107), .audio (p. 108)

B

.band (p. 108), .bargains (p. 109), .bike (p. 110), .bingo (p. 110), .biz (p. 111), .black (p. 112), .blue (p. 112), .boutique (p. 113), .builders (p. 114), .business (p. 114), .buzz (p. 115)

C

.cab (p. 116), .cafe (p. 116), .camera (p. 117), .camp (p. 118), .capital (p. 118), .cards (p. 119), .care (p. 120), .careers (p. 120), .cash (p. 121), .casino (p. 122), .catering (p. 122), .cc (p. 123), .center (p. 123), .ceo (p. 124), .chat (p. 124), .cheap (p. 125), .church (p. 126), .city (p. 126), .claims (p. 127), .cleaning (p. 128), .click (p. 128), .clinic (p. 129), .clothing (p. 130), .cloud (p. 130), .club (p. 131), .coach (p. 132), .codes (p. 132), .coffee (p. 133), .college (p. 134), .com (p. 134), .community (p. 135), .company (p. 136), .computer (p. 136), .condos (p. 137), .construction (p. 138), .consulting (p. 138), .contractors (p. 139), .cool (p. 140), .coupons (p. 140), .credit (p. 141), .creditcard (p. 142), .cruises (p. 142)

D

.dance (p. 143), .dating (p. 144), .deals (p. 144), .delivery (p. 145), .democrat (p. 146), .dental (p. 146), .diamonds (p. 147), .diet (p. 148), .digital (p. 148), .direct (p. 149), .directory (p. 150), .discount (p. 150), .dog (p. 151), .domains (p. 152)

E

.education (p. 152), .email (p. 153), .energy (p. 154), .engineering (p. 154), .enterprises (p. 155), .equipment (p. 156), .estate (p. 156), .events (p. 157), .exchange (p. 158), .expert (p. 158), .exposed (p. 159), .express (p. 160)

F

.fail (p. 160), .farm (p. 161), .finance (p. 162), .financial (p. 162), .fish (p. 163),
.fitness (p. 164), .flights (p. 164), .florist (p. 165), .flowers (p. 166), .fm (p. 166),
.football (p. 166), .forsale (p. 167), .foundation (p. 168), .fund (p. 168), .furniture (p. 169),
.futbol (p. 170), .fyi (p. 170)

G

.gallery (p. 171), .gift (p. 172), .gifts (p. 172), .glass (p. 173), .global (p. 174), .gold (p. 174),
.golf (p. 175), .graphics (p. 176), .gratis (p. 176), .green (p. 177), .gripe (p. 178),
.guide (p. 178), .guitars (p. 179), .guru (p. 180)

H

.haus (p. 180), .healthcare (p. 181), .help (p. 182), .hiv (p. 182), .hockey (p. 183),
.holdings (p. 184), .holiday (p. 184), .host (p. 185), .hosting (p. 186), .house (p. 186)

I

.im (p. 187), .immo (p. 187), .immobilien (p. 188), .industries (p. 188), .info (p. 189),
.ink (p. 190), .institute (p. 190), .insure (p. 191), .international (p. 192), .investments (p. 192),
.io (p. 193), .irish (p. 193)

J

.jewelry (p. 194), .juegos (p. 194)

K

.kaufen (p. 195), .kim (p. 196), .kitchen (p. 196), .kiwi (p. 197)

L

.land (p. 198), .lease (p. 198), .legal (p. 199), .lgbt (p. 200), .life (p. 200), .lighting (p. 201),
.limited (p. 202), .limo (p. 202), .link (p. 203), .live (p. 204), .loan (p. 204), .loans (p. 205),
.lol (p. 206)

M

.maison (p. 206), .management (p. 207), .marketing (p. 208), .mba (p. 208), .media (p. 209),
.memorial (p. 210), .mobi (p. 210), .moda (p. 211), .money (p. 212), .mortgage (p. 212),
.movie (p. 213)

N

.name (p. 214), .net (p. 214), .network (p. 215), .news (p. 216), .ninja (p. 216)

O

.onl (p. 217), .online (p. 218), .org (p. 218)

P

.partners (p. 219), .parts (p. 220), .photo (p. 220), .photography (p. 221), .photos (p. 222),
.pics (p. 222), .pictures (p. 223), .pink (p. 224), .pizza (p. 224), .place (p. 225),
.plumbing (p. 226), .plus (p. 226), .poker (p. 227), .porn (p. 228), .pro (p. 228),
.productions (p. 229), .properties (p. 230), .property (p. 230), .pub (p. 231)

Q

.qpon (p. 232)

R

.recipes (p. 232), .red (p. 233), .reise (p. 234), .reisen (p. 234), .rentals (p. 235),
.repair (p. 236), .report (p. 236), .republican (p. 237), .restaurant (p. 238), .reviews (p. 238),
.rip (p. 239), .rocks (p. 240), .run (p. 240)

S

.sale (p. 241), .sarl (p. 242), .school (p. 242), .schule (p. 243), .services (p. 244), .sex (p. 244), .sexy (p. 245), .shiksha (p. 246), .shoes (p. 246), .show (p. 247), .singles (p. 248), .soccer (p. 248), .social (p. 249), .solar (p. 250), .solutions (p. 250), .studio (p. 251), .style (p. 252), .sucks (p. 252), .supplies (p. 253), .supply (p. 254), .support (p. 254), .surgery (p. 255), .systems (p. 256)

T

.tattoo (p. 256), .tax (p. 257), .taxi (p. 258), .team (p. 258), .technology (p. 259), .tennis (p. 260), .theater (p. 260), .tienda (p. 261), .tips (p. 262), .tires (p. 262), .today (p. 263), .tools (p. 264), .tours (p. 264), .town (p. 265), .toys (p. 266), .trade (p. 266), .training (p. 267), .tv (p. 268)

U

.university (p. 268), .uno (p. 269)

V

.vacations (p. 270), .vegas (p. 270), .ventures (p. 271), .vg (p. 272), .viajes (p. 272), .video (p. 272), .villas (p. 273), .vision (p. 274), .voyage (p. 274)

WXYZ

.watch (p. 275), .website (p. 276), .wiki (p. 276), .works (p. 277), .world (p. 278), .wtf (p. 278), .xyz (p. 279), .zone (p. 280)

.ac

See [.ac \(Ascension Island\) \(p. 281\)](#).

[Return to index](#)

.academy

Used by educational institutions such as schools and universities. Also used by recruiters, advisors, advertisers, students, teachers, and administrators who are affiliated with educational institutions.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.accountants

Used by businesses, groups, and individuals affiliated with the accounting profession.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.adult

Used for websites that host adults-only content.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.agency

Used by any businesses or groups that identify as agencies.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.apartments

Used by real estate agents, landlords, and renters.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.associates

Used by businesses and firms that include the term "associates" in their titles. Also used by any groups or agencies that want to indicate the professional nature of their organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.auction

Used for events related to auctions and auction-based buying and selling.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Spanish, and Latin.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.audio

Important

You can no longer use Route 53 to register new .audio domains or transfer .audio domains to Route 53. We'll continue to support .audio domains that are already registered with Route 53.

Used by the audiovisual industry and anyone interested in broadcasting, sound equipment, audio production, and audio streaming.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .audio domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.band

Used for sharing information about musical bands and band events. Also used by musicians to connect with their fan base and sell band-related merchandise.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Spanish, and Latin.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.bargains

Used for information about sales and promotions.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.bike

Used by businesses or groups that cater to cyclists, such as bike stores, motorcycle dealerships, and repair shops.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.bingo

Used for online gaming websites or for sharing information about the game of bingo.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.biz

Used for business or commercial use.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Simplified Chinese, Traditional Chinese, Danish, Finnish, German, Hungarian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Spanish, and Swedish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.black

Used by those who like the color black or those who want to associate the color black with their business or brand.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.blue

Used by those who like the color blue or those who want to associate the color blue with their business or brand.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.boutique

Used for information about boutiques and small specialty shops.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.builders

Used by companies and individuals affiliated with the construction industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.business

Used by any kind of business. Can be used as an alternative to the .biz extension.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.buzz

Used for information about the latest news and events.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cab

Used by companies and individuals affiliated with the taxicab industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cafe

Used by cafe businesses and those who have an interest in cafe culture.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.camera

Used by photography enthusiasts and anyone who wants to share photos.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.camp

Used by parks and recreation departments, summer camps, writers' workshops, fitness camps, and camping enthusiasts.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.capital

Used as a general category that describes any kind of capital, such as financial capital or the capital of a city.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cards

Used by businesses that specialize in cards such as ecards, printed greeting cards, business cards, and playing cards. Also ideal for gamers who want to discuss the rules and strategies of card games.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.care

Used by businesses or agencies in the care-giving field. Also used by charitable organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.careers

Used for information about job recruitment.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cash

Used by any organization, group, or individual engaged in money-related activities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.casino

Used by the gambling industry or by gamers who want to share information about gambling and casino games.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.catering

Used by catering businesses or those who share information about food-related events.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.CC

See [.cc \(Cocos \(Keeling\) Islands\) \(p. 294\)](#).

[Return to index](#)

.center

Used as a generic extension for everything from research organizations to community centers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.ceo

Used for information about CEOs and their equals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for German.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.chat

Used by any kind of online chat website.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cheap

Used by e-commerce websites to promote and sell inexpensive products.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.church

Used by churches of any size or denomination to connect with their congregations and to publish information about church-related events and activities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.city

Used to provide information about specific cities, such as points of interest, top local spots to visit, or neighborhood activities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.claims

Used by companies that handle insurance claims or provide legal services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cleaning

Used by businesses or individuals that provide cleaning services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.click

Used by businesses that want to associate the action of clicking with their websites, for example, clicking products on a website to purchase them.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.clinic

Used by the health care industry and by medical professionals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.clothing

Used by those in the fashion industry, including retailers, department stores, designers, tailors, and outlets.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cloud

Used as a general extension, but ideal for companies that provide cloud computing technologies and services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.club

Used by any type of club or organization.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Spanish and Japanese.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.coach

Used by anyone with an interest in coaching, such as sports professionals, lifestyle coaches, or corporate trainers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.codes

Used as a generic extension for all kinds of code, such as codes of conduct, building codes, or programming code.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.coffee

Used by those in the coffee industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.college

Used by educational institutions such as schools and universities. Also used by recruiters, advisors, advertisers, students, teachers, and administrators who are affiliated with educational institutions.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, simplified and traditional Chinese, Cyrillic, Greek, Hebrew, Japanese, and Thai.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.com

Used for commercial websites. It is the most popular extension on the internet.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is Amazon Registrar, Inc.

.community

Used by any type of community, club, organization, or special interest group.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.company

Used as a generic extension for companies of all kinds.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.computer

Used as a generic extension for information about computers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.condos

Used by individuals and businesses associated with condominiums.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.construction

Used by those in the construction industry, such as builders and contractors.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.consulting

Used by consultants and others who are affiliated with the consulting industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Chinese, French, Cyrillic, Devanagari, German, Greek, Hebrew, Japanese, Korean, Latin, Spanish, Tamil, and Thai.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.contractors

Used by contractors, such as contractors in the construction industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cool

Used by organizations and groups who want to associate their brand with the latest trends.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.coupons

Used by retailers and manufacturers that provide online coupons and coupon codes.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.credit

Used by the credit industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.creditcard

Used by companies or banks that issue credit cards.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.cruises

Used by the voyage industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.dance

Used by dancers, dance instructors, and dance schools.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.dating

Used for dating websites.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.deals

Used to provide information about online bargains and sales.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.delivery

Used by companies that deliver any kind of merchandise or service.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.democrat

Used for information about the Democratic Party. Also used by officials running for elected office, elected officials, political enthusiasts, consultants, and advisors.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.dental

Used by dental professionals and dental suppliers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.diamonds

Used by diamond enthusiasts and those in the diamond industry, including sellers, resellers, and merchandisers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.diet

Important

You can no longer use Route 53 to register new .diet domains or transfer .diet domains to Route 53. We'll continue to support .diet domains that are already registered with Route 53.

Used by health and fitness professionals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .diet domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.digital

Used for anything and everything digital, but ideal for technology businesses.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.direct

Used as a general extension, but ideal for those who sell products directly to customers through an e-commerce website.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.directory

Used by the media sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.discount

Used for discount websites and businesses that slash prices.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.dog

Used by dog lovers and those who provide canine services and products.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.domains

Used for information about domain names.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.education

Used for information about education.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.email

Used for information about promoting email.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.energy

Used as a general extension, but ideal for those in the energy or energy conservation fields.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.engineering

Used by engineering firms and professionals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.enterprises

Used for information about enterprises and businesses.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.equipment

Used for information about equipment, equipment retailers or manufacturers, and rental shops.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.estate

Used for information about housing and the housing sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.events

Used for information about events of all kinds.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.exchange

Used for any type of exchange: the stock exchange, the exchange of goods, or even the simple exchange of information.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.expert

Used by those who have specialized knowledge in a variety of fields.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.exposed

Used as a generic extension for a variety of subjects, including photography, tabloids, and investigative journalism.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.express

Used as a general extension, but ideal for those who want to emphasize the speedy delivery of good or services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fail

Used by anyone who has made mistakes, but ideal for publishing humorous "fail" blunders and bloopers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.farm

Used by those in the farming industry, such as farmers and agricultural engineers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.finance

Used by the financial sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.financial

Used by the financial sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fish

Used as a general extension, but ideal for websites related to fish and fishing.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fitness

Used to promote fitness and fitness services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.flights

Used by travel agents, airlines, and anyone affiliated with the travel industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.florist

Used by florists.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.flowers

Important

You can no longer use Route 53 to register new .flowers domains or transfer .flowers domains to Route 53. We'll continue to support .flowers domains that are already registered with Route 53.

Used for anything related to flowers, such as online flower sales or information about flower growing and breeding.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .flowers domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fm

See [.fm \(Federated States of Micronesia\) \(p. 298\)](#).

[Return to index](#)

.football

Used by anyone involved in the sport of football.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.forsale

Used for selling goods and services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.foundation

Used by non-profit organizations, charities, and other kinds of foundations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fund

Used as a general extension for anything related to funding.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.furniture

Used by furniture makers and sellers and anyone affiliated with the furniture industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.futbol

Used for information about soccer (futbol).

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fyi

Used as a general extension, but ideal for sharing information of all kinds. "FYI" is an acronym for "for your information."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.gallery

Used by owners of art galleries.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.gift

Used by businesses or organizations that sell gifts or provide gift-related services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.gifts

Used by businesses or organizations that sell gifts or provide gift-related services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.glass

Used by those in the glass industry, such as glass cutters and window installers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.global

Used by businesses or groups with an international market or vision.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Belarusian, Bosnian, Bulgarian, Chinese (Simplified) Chinese (Traditional), Danish, German, Hindi, Hungarian, Icelandic, Korean, Latvian, Lithuanian, Macedonian, Montenegrin, Polish, Russian, Serbian, Spanish, Swedish, and Ukrainian.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.gold

Used as a general extension, but ideal for companies that purchase or sell gold or gold-related products.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.golf

Used for websites devoted to the game of golf.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.graphics

Used by those in the graphics industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.gratis

Used for websites that offer free products, such as promotional items, downloads, or coupons. "Gratis" is a Spanish word that means "free."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.green

Used for websites devoted to conservation, ecology, the environment, and the green lifestyle.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.gripe

Used for sharing complaints and criticism.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.guide

Used as a general extension, but ideal for websites that focus on travel destinations, services, and products.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.guitars

Important

You can no longer use Route 53 to register new .guitars domains or transfer .guitars domains to Route 53. We'll continue to support .guitars domains that are already registered with Route 53.

Used by guitar enthusiasts.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .guitars domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.guru

Used by those who want to share their knowledge about a variety of subjects.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.haus

Used by real estate and construction industries. "Haus" is a German word that means "house."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.healthcare

Used by the healthcare sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.help

Used as a general extension, but ideal for websites that provide online help and information.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.hiv

Used for websites devoted to the fight against HIV.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.hockey

Used for websites devoted to the game of hockey.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.holdings

Used by financial advisors, stockbrokers, and those who work with investments.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.holiday

Used by those in the travel industry and individuals and businesses involved in party planning and special occasions.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.host

Used by companies that provide web hosting platforms and services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Simplified Chinese, Traditional Chinese, Greek, Hebrew, Korean, and Thai.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.hosting

Important

You can no longer use Route 53 to register new .hosting domains or transfer .hosting domains to Route 53. We'll continue to support .hosting domains that are already registered with Route 53.

Used for hosting websites or by those in the hosting industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .hosting domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.house

Used by real estate agents and buyers and sellers of houses.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.im

See [.im \(Isle of Man\) \(p. 316\)](#).

[Return to index](#)

.immo

Used by the real estate sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.immobilien

Used for information about real estate.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.industries

Used by any business or commercial enterprise that wants to identify as an industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.info

Used for the dissemination of information.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.ink

Used by tattoo enthusiasts or any industry related to ink, such as printing and publishing industries.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic and Latin.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.institute

Used by any organization or group, especially research and educational organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.insure

Used by insurance companies and insurance brokers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.international

Used by businesses that have international chains, individuals who travel internationally, or charity organizations with an international influence.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.investments

Used as a general extension, but ideal for promoting investment opportunities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.io

See [.io \(British Indian Ocean Territory\) \(p. 300\)](#).

[Return to index](#)

.irish

Used for promoting Irish culture and organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Simplified Chinese, Traditional Chinese, French, German, Greek, Hebrew, Japanese, Korean, Spanish, Tamil, and Thai.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

jewelry

Used by jewelry sellers and buyers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

juegos

Important

You can no longer use Route 53 to register new .juegos domains or transfer .juegos domains to Route 53. We'll continue to support .juegos domains that are already registered with Route 53.

Used for gaming websites of all kinds. "Juegos" is a Spanish word that means "games."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .juegos domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.kaufen

Used for information about e-commerce.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.kim

Used by people whose name or surname is Kim.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.kitchen

Used by kitchen retailers, cooks, food bloggers, and anyone in the food industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.kiwi

Used by companies and individuals who want to support New Zealand kiwi culture. It is also used as a platform for charitable aid in the reconstruction of Christchurch, damaged by earthquakes in 2010 and 2011.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Maori.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.land

Used by farmers, real estate agents, commercial developers, and anyone with an interest in property.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.lease

Used by realtors, landlords, and renters.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.legal

Used by members of the legal profession.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.lgbt

Used by the community of lesbian, gay, bisexual, and transgender people.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.life

Used as a general extension, and suitable for a wide range of businesses, groups, and individuals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.lighting

Used by photographers, designers, architects, engineers, and others with an interest in lighting.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.limited

Used as a general extension, and suitable for a wide range of businesses, groups, and individuals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.limo

Used by chauffeurs, limousine companies, and car rental agencies.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.link

Used for information about the creation of online shortcut links.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Supported, but you must open a case with AWS Support and request that they enable or disable privacy protection for your domains. When you open the case, specify the domain names in the **Description** field. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.live

Used as a general extension, and suitable for a wide range of businesses, groups, and individuals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.loan

Used by lenders, borrowers, and credit professionals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Danish, German, Norwegian, and Swedish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.loans

Used by lenders, borrowers, and credit professionals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.lol

Used for humor and comedy websites. "LOL" is an acronym for "laugh out loud."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic, French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.maison

Used by the real estate sector.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.management

Used for information about the business world and company management.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration

- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.marketing

Used by the marketing sector for a variety of purposes.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.mba

Used for websites that provide information about the master's degree in business administration (MBA).

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.media

Used by the media and entertainment sectors.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.memorial

Used by commemorative organizations dedicated to honoring events and people.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.mobi

Used by companies and individuals who want to have their websites accessible on mobile phones.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.moda

Used for information about fashion.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.money

Used for websites that focus on money and money-related activities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.mortgage

Used by the mortgage industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.movie

Used for websites that provide information about movies and movie-making. Suitable for both professionals and fans.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.name

Used by anyone who wants to create a personalized web presence.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Verisign, the registry for .name TLDs, allows you to register both second-level domains (*name.name*) and third-level domains (*firstname.lastname.name*). Route 53 supports only second-level domains, both for registering domains and for transferring existing domains to Route 53.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.net

Used for all types of websites. The .net extension is an abbreviation of network.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is Amazon Registrar, Inc.

.network

Used by those in the network industry or those who want to build connections through networking.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.news

Used for distributing any newsworthy information such as current events or information related to journalism and communication.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.ninja

Used by individuals and businesses who want to associate themselves with the abilities of a ninja.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.onl

The .onl extension is an abbreviation for "online," and it is also the short term in Spanish for non-profit organization.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Belarusian, Bosnian, Bulgarian, Chinese (Simplified and Traditional), Danish, German, Hindi, Hungarian, Icelandic, Korean, Lithuanian, Latvian, Macedonian, Polish, Russian, Serbian, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.online

The .onl extension is an abbreviation for "online," and it is also the short term in Spanish for non-profit organization.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.org

Used by all kinds of organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is Amazon Registrar, Inc.

.partners

Used by law firms, investors, and a variety of companies. Also used for social websites that build relationships.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.parts

Used as a general extension, but ideal for parts manufacturers, sellers, and buyers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.photo

Used by photographers and anyone interested in photos.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.photography

Used by photographers and anyone interested in photos.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.photos

Used by photographers and anyone interested in photos.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.pics

Used by photographers and anyone interested in photos.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.pictures

Used by anyone interested in photography, art, and media.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.pink

Used by those who like the color pink or those who want to associate the color pink with their business or brand.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.pizza

Used by pizza restaurants and pizza lovers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.place

Used as a general extension, but ideal for the home and travel sectors.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.plumbing

Used by those in the plumbing industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.plus

Used as a general extension, but ideal for plus-size clothing, add-on software, or any product that offers "extra" features or dimensions.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.poker

Used by poker players and gaming websites.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.porn

Used for adults-only websites.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.pro

Used by licensed and credentialed professionals and professional organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.productions

Used by studios and production houses that make commercials, radio ads, and music videos.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.properties

Used for information about any type of property, including real estate or intellectual property. Also used by those who have houses, buildings, or land to sell, lease, or rent.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.property

Important

You can no longer use Route 53 to register new .property domains or transfer .property domains to Route 53. We'll continue to support .property domains that are already registered with Route 53.

Used for information about any type of property, including real estate or intellectual property. Also used by those who have houses, buildings, or land to sell, lease, or rent.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .property domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.pub

Used by those in the publication, advertising, or brewing business.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.qpon

Used for coupons and promo codes.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.recipes

Used by those with recipes to share.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.red

Used by those who like the color red or those who want to associate the color red with their business or brand.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.reise

Used for websites related to travels or journeys. "Reise" is a German word that means "rise," "arise," or "set out on a journey."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.reisen

Used for websites related to travels or journeys. "Reisen" is a German word that means "to travel."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.rentals

Used for all types of rentals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.repair

Used by repair services or by those who want to teach others how to repair all kinds of items.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.report

Used as a general extension, but ideal for information about business reports, community publications, book reports, or news reporting.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.republican

Used for information about the Republican Party. Also used by officials running for elected office, elected officials, political enthusiasts, consultants, and advisors.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date

- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.restaurant

Used by the restaurant industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.reviews

Used by those who want give their opinions and read the comments of others.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.rip

Used for websites dedicated to death and memorials. "RIP" is an acronym for "rest in peace."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.rocks

Used as a general extension, but ideal for anyone who "rocks": musicians, geologists, jewelers, climbers, and more.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.run

Used as a general extension, but ideal for the fitness and sports industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.sale

Used by e-commerce websites.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.sarl

Used by limited liability companies typically located in France. "SARL" is an acronym for Société à Responsabilité Limitée.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.school

Used for information about education, educational institutions, and school-related activities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.schule

Used for information about German-based education, educational institutions, and school-related activities. "Schule" is a German word that means "school."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.services

Used for websites that focus on services of any kind.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.sex

Used for adults-only content.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.sexy

Used for sexual content. Also used for describing the most popular and exciting brands, products, information, and websites.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.shiksha

Used by educational institutions. "Shiksha" is an Indian term for school.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.shoes

Used by shoe retailers, designers, manufacturers, or fashion bloggers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.show

Used as a general extension, but ideal for the entertainment industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.singles

Used by dating services, resorts, and other businesses that cater to those who want to make a connection.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.SOCCER

Used for websites dedicated to the game of soccer.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.social

Used for information about social media, forums, and online conversations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.solar

Used for information about the solar system or solar energy.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.solutions

Used by consultants, do-it-yourself services, and advisors of all kinds.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.studio

Used as a general extension, but ideal for those in the real estate, art, or entertainment industries.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

[.style](#)

Used as a general extension, but ideal for websites dedicated to the latest trends, especially trends in fashion, design, architecture, and art.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

[.sucks](#)

Used as a general extension, but ideal for those who want to share negative experiences or warn others about scams, frauds, or faulty products.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.supplies

Used by businesses that sell goods online.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.supply

Used by businesses that sell goods online.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.support

Used by businesses, groups, or charities that offer any kind of support, including customer, product, or system support or emotional, financial, or spiritual support.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.surgery

Used for information about surgery, medicine, and healthcare.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.systems

Used primarily by the technology industry and those who offer technology services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tattoo

Used by tattoo enthusiasts and the tattoo industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Cyrillic (primarily Russian), French, German, Italian, Portuguese, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tax

Used for information about taxes, tax preparation, and tax law.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.taxi

Used by cab, chauffeur, and shuttle companies.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.team

Used by any business or organization that wants to identify as a team.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.technology

Used by technology enthusiasts and those dedicated to technology in companies, services, and manufacturers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tennis

Used for information related to the game of tennis.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.theater

Used for websites dedicated to theaters, plays, and musicals.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tienda

Used by retail businesses that want to connect with Spanish-speaking consumers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tips

Used by those who want to share their knowledge and advice on virtually any topic.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tires

Used by manufacturers, distributors, or buyers of tires.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.today

Used for information about current events, news, weather, entertainment, and more.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tools

Used for information about any kind of tool.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tours

Used as a general extension, but ideal for travel companies.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.town

Used to promote a city's locale, culture, and community.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.toys

Used by the toy industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.trade

Used as a general extension, but ideal for commerce websites or trading services.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Danish, German, Norwegian, and Swedish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.training

Used by trainers, coaches, and educators.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.tv

Used for information about television and media.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Domain names that are at least three letters long (such as aaa.tv) are generally open to the public. Wwww.tv, the registry for .tv domains, reserves two-letter domain names. You can't register two-letter domains with or transfer them to Route 53. For more information about .tv domain names, see the [.tv page](#) on the Verisign website.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.university

Used by universities and other educational organizations.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.UNO

Used for information about the Hispanic, Portuguese, and Italian communities.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.vacations

Used by the travel and tourism industry.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.vegas

Used to promote the city of Las Vegas and the Las Vegas lifestyle.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.ventures

Used by entrepreneurs, startups, venture capitalists, investment banks, and financiers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.vg

See [.vg \(British Virgin Islands\) \(p. 290\)](#).

[Return to index](#)

.viajes

Used by travel agencies, tour operators, travel blogs, tour companies, rental services, travel bloggers, and travel retailers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.video

Used by media and video industries.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Chinese, French, German, Latin, and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.villas

Used by real estate agents and property owners who have villas to sell, rent, or lease.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.vision

Used as a general extension, but ideal for vision specialists such as optometrists and ophthalmologists.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.voyage

Used by travel agencies, tour operators, travel blogs, tour companies, rental services, travel bloggers, and travel retailers.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.watch

Used for information about streaming websites, web TVs, video, or watches.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration

- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.website

Used for information about website development, promotion, improvements, and experiences.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Simplified Chinese, Traditional Chinese, Greek, Hebrew, Japanese, Korean, and Thai.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.wiki

Used for information about online documentation.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic and Latin.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.works

Used by businesses, organizations, and individuals for information about work, job, and employment services. This extension can be used as an alternative to the .com, .net, or .org extensions.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration

- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.world

Used by anyone who wants to provide information about global subjects.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.wtf

Used by anyone who wants to identify with the popular (but profane) acronym "WTF."

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.xyz

Used as a general extension for any purpose.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

The registry for .xyz domains, Generation XYZ, considers some domain names to be premium domain names. You can't register premium .xyz domains with or transfer them to Route 53. For more information, see the [Generation XYZ](#) website.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.zone

Used for information about any kind of zone, including time zones, climate zones, and sports zones.

[Return to index](#)

Registration and renewal period

One to ten years.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden except organization name.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for French and Spanish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Geographic top-level domains

The following domain extensions are grouped by geography and include official country-specific extensions, known as *country code top-level domains* (ccTLDs). Examples include .be (Belgium), .in (India), and .mx (Mexico). The rules for registration of ccTLDs vary by country. Some countries are unrestricted, meaning that anyone in the world can register, while others have certain restrictions, such as residency. The listing for each ccTLD indicates any restrictions.

[Return to index](#)

Africa

[.ac \(Ascension Island\) \(p. 281\)](#), [.co.za \(South Africa\) \(p. 282\)](#), [.sh \(Saint Helena\) \(p. 283\)](#)

Americas

[.ca \(Canada\) \(p. 284\)](#), [.cl \(Chile\) \(p. 285\)](#), [.co \(Colombia\) \(p. 286\)](#), [.com.ar \(Argentina\) \(p. 286\)](#), [.com.br \(Brazil\) \(p. 287\)](#), [.com.mx \(Mexico\) \(p. 288\)](#), [.mx \(Mexico\) \(p. 288\)](#), [.us \(United States\) \(p. 289\)](#), [.vc \(Saint Vincent and the Grenadines\) \(p. 290\)](#), [.vg \(British Virgin Islands\) \(p. 290\)](#)

Asia/Oceania

[.au \(Australia\) \(p. 291\)](#), [.cc \(Cocos \(Keeling\) Islands\) \(p. 294\)](#), [.co.nz \(New Zealand\) \(p. 295\)](#), [.com.au \(Australia\) \(p. 295\)](#), [.com.sg \(Republic of Singapore\) \(p. 297\)](#), [.fm \(Federated States of Micronesia\) \(p. 298\)](#), [.in \(India\) \(p. 298\)](#), [.jp \(Japan\) \(p. 299\)](#), [.io \(British Indian Ocean Territory\) \(p. 300\)](#), [.net.au \(Australia\) \(p. 301\)](#), [.net.nz \(New Zealand\) \(p. 302\)](#), [.org.nz \(New Zealand\) \(p. 303\)](#), [.qa \(Qatar\) \(p. 304\)](#), [.ru \(Russian Federation\) \(p. 305\)](#), [.sg \(Republic of Singapore\) \(p. 306\)](#)

Europe

[.be \(Belgium\) \(p. 307\)](#), [.berlin \(city of Berlin in Germany\) \(p. 307\)](#), [.ch \(Switzerland\) \(p. 308\)](#), [.co.uk \(United Kingdom\) \(p. 309\)](#), [.cz \(Czech Republic\) \(p. 310\)](#), [.de \(Germany\) \(p. 310\)](#), [.es \(Spain\) \(p. 311\)](#), [.eu \(European Union\) \(p. 312\)](#), [.fi \(Finland\) \(p. 313\)](#), [.fr \(France\) \(p. 314\)](#), [.gg \(Guernsey\) \(p. 315\)](#), [.im \(Isle of Man\) \(p. 316\)](#), [.it \(Italy\) \(p. 316\)](#), [.me \(Montenegro\) \(p. 317\)](#), [.me.uk \(United Kingdom\) \(p. 318\)](#), [.nl \(the Netherlands\) \(p. 319\)](#), [.org.uk \(United Kingdom\) \(p. 320\)](#), [.ruhr \(Ruhr region, western part of Germany\) \(p. 321\)](#), [.se \(Sweden\) \(p. 321\)](#), [.uk \(United Kingdom\) \(p. 322\)](#), [.wien \(city of Vienna in Austria\) \(p. 323\)](#)

Africa

You can use the following top-level domains (TLDs) for Africa to register domains with Amazon Route 53.

the section called “[.ac \(Ascension Island\)](#)”, the section called “[.co.za \(South Africa\)](#)”, the section called “[.sh \(Saint Helena\)](#)”

[Return to index](#)

[.ac \(Ascension Island\)](#)

[Return to index](#)

Also used as a generic TLD that is popular for those in academia.

Registration and renewal period

One year.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Determined by the registry.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.co.za (South Africa)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Only second-level domains are available for the .za extension. Route 53 supports the second-level domain .co.za.

Open to the public, with some restrictions:

- Registration is open to identifiable legal entities (individuals and legal persons).
- The domain name must pass a zone check during the registration process.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

No

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until one day before the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: 1 day before expiration
- Restoration with the registry is possible: Between 1 day and 9 days after expiration
- Domain is deleted from the registry: 9 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.sh (Saint Helena)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Americas

You can use the following top-level domains (TLDs) for the Americas to register domains with Amazon Route 53.

[the section called ".ca \(Canada\)",](#) [the section called ".cl \(Chile\)",](#) [the section called ".co \(Colombia\)",](#) [the section called ".com.ar \(Argentina\)",](#) [the section called ".com.br \(Brazil\)",](#) [the section called ".com.mx](#)

(Mexico)", the section called ".mx (Mexico)", the section called ".us (United States)", the section called ".vc (Saint Vincent and the Grenadines)", the section called ".vg (British Virgin Islands)"

[Return to index](#)

.ca (Canada)

[Return to index](#)

Confirmation email from the TLD registry

When you register a .ca domain, you will receive an email with a link to the acceptance procedure of the registrant agreement. You must complete the procedure within seven days or your domain will not be registered.

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with some restrictions:

- Registration is open to individuals or organizations connected to Canada, as described by the Canadian Presence Requirements for Registrants.
- Registrant contact: You must provide the full and exact legal name of the owner of the domain.
- Admin and tech contacts: You must specify **Person** as the contact type and provide contact information for individuals living in Canada.
- You must select one of the following legal types during the registration process:
 - ABO: Aboriginal Peoples (individuals or groups) indigenous to Canada
 - ASS: Canadian unincorporated association
 - CCO: Canadian corporation, or Canadian province or territory
 - CCT: Canadian citizen
 - EDU: Canadian educational institution
 - GOV: Government or government entity in Canada
 - HOP: Canadian hospital
 - INB: Indian Band recognized by the Indian Act of Canada
 - LAM: Canadian library, archive, or museum
 - LGR: Legal Representative of a Canadian Citizen or Permanent Resident
 - MAJ: Her/His Majesty the Queen/King
 - OMK: Official mark registered in Canada
 - PLT: Canadian political party
 - PRT: Partnership registered in Canada
 - RES: Permanent resident of Canada
 - TDM: Trade-mark registered in Canada (by a non-Canadian owner type)
 - TRD: Canadian trade union
 - TRS: Trust established in Canada

Privacy protection

- **Person** – For all contacts, contact name, address, phone number, fax number, and email address are hidden.
- **Company, association, or public body** – Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: Varies. Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .ca domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

.cl (Chile)

Important

You can no longer use Route 53 to register new .cl domains or transfer .cl domains to Route 53. We'll continue to support .cl domains that are already registered with Route 53.

[Return to index](#)

Renewal period

Two years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .cl domains to Route 53.

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Contact [AWS Support](#).
- Late renewal with Route 53 is possible: Contact [AWS Support](#).

- Domain is deleted from Route 53: Contact [AWS Support](#).
- Restoration with the registry is possible: Contact [AWS Support](#).
- Domain is deleted from the registry: Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.co (Colombia)

[Return to index](#)

Registration and renewal period

One to five years.

Restrictions

The registry for .co domains, Go.co, considers some domain names to be premium domain names. You can't register premium .co domains with or transfer them to Route 53. For more information, see the [Go.co](#) website.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: Between 30 days and 45 days after expiration
- Domain is deleted from the registry: 50 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.com.ar (Argentina)

Important

You can no longer use Route 53 to register new .com.ar domains or transfer .com.ar domains to Route 53. We'll continue to support .com.ar domains that are already registered with Route 53.

[Return to index](#)

Renewal period

One year.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .com.ar domains to Route 53.

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Contact [AWS Support](#).
- Late renewal with Route 53 is possible: Contact [AWS Support](#).
- Domain is deleted from Route 53: Contact [AWS Support](#).
- Restoration with the registry is possible: Contact [AWS Support](#).
- Domain is deleted from the registry: Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.com.br (Brazil)

Important

You can no longer use Route 53 to register new .com.br domains or transfer .com.br domains to Route 53. We'll continue to support .com.br domains that are already registered with Route 53.

[Return to index](#)

Renewal period

One year.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .com.br domains to Route 53.

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Between 30 days before expiration and the expiration date
- Late renewal with Route 53 is possible: Until 119 days after expiration
- Domain is deleted from Route 53: 119 days after expiration
- Restoration with the registry is possible: No

- Domain is deleted from the registry: 119 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.com.mx (Mexico)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Determined by the registry.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.mx (Mexico)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Determined by the registry.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 75 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.us (United States)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

The registry for .us domains doesn't allow domain names that contain any of the seven words identified in the "Appendix to Opinion of the Court" of [Federal Communications Commission v. Pacifica Foundation No. 77-528](#).

Open to the public, with one restriction:

- The .us extension is for websites or activities that are located in the United States of America.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: Between 30 days and 60 days after expiration
- Domain is deleted from the registry: 65 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.vc (Saint Vincent and the Grenadines)

Also used as a generic TLD, often by those involved in venture capital financing, varsity colleges, and so on.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection (applies to all contact types: person, company, association, and public body)

All information is hidden.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.vg (British Virgin Islands)

Also used as a generic TLD, often by organizations involved in video gaming.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until 44 days after the expiration date
- Late renewal with Route 53 is possible: Yes
- Domain is deleted from Route 53: 45 days after expiration
- Domain is deleted from the registry: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 74 days after expiration
- Domain is made publicly available again: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Asia/Oceania

You can use the following top-level domains (TLDs) for Asia and Oceania to register domains with Amazon Route 53.

the section called ".au (Australia)", the section called ".cc (Cocos (Keeling) Islands)", the section called ".co.nz (New Zealand)", the section called ".com.au (Australia)", the section called ".com.sg (Republic of Singapore)", the section called ".fm (Federated States of Micronesia)", the section called ".in (India)", the section called ".jp (Japan)", the section called ".io (British Indian Ocean Territory)", the section called ".net.au (Australia)", the section called ".net.nz (New Zealand)", the section called ".org.nz (New Zealand)", the section called ".qa (Qatar)", the section called ".ru (Russian Federation)", the section called ".sg (Republic of Singapore)"

[Return to index](#)

.au (Australia)

[Return to index](#)

Note

.au domain registration is coming soon! auDA, the registry for the .au top-level domain (TLD) has announced that .au TLD registration will be available starting 24 March 2022. The registration process for .au domain will be same as other domains unless another party owns

the corresponding second-level domain (SLD) of .au (for example, .com.au or net.au). For the owners of those .au SLD domains, there will be a priority registration period open from March 24 until September 20, 2022. For more information, see [The Priority Allocation Process](#) and the [FAQ for .au domains \(p. 293\)](#).

Confirmation email from the TLD registry

Our registrar associate, Gandi, resells .au domains through DomainDirectors. When you transfer a domain name to Route 53, DomainDirectors sends an email to the registrant contact for the domain to verify contact information or to authorize transfer requests.

Registration and renewal period

One to five years.

Restrictions

Open to the public, with some restrictions:

- The .au domains are open to legal persons, trading, partnerships, or sole traders registered in Australia; to foreign companies licensed to trade in Australia; and to owners or applicants of an Australian-registered trademark. Individuals cannot register .au domains. The registrant contact must be a company.
- Your domain name must be identical to your name, as registered with the relevant Australian authorities or to your trademark (or to the abbreviation or acronym).
- The domain name should indicate your activity. For example, it should indicate a product that you sell or a service that you provide.
- During the registration process, you must indicate the following:
 - Your registration type: ABN (Australian Business Number), ACN (Australian Company Number), or TM (Trademark) if the domain name corresponds to your trademark.
 - Your ID number, which can be a Medicare card number, a tax file number (TFN), a state driver's license number, or an Australian Business Number (ABN).
 - Your state or province.
- Incorrect or mismatched contact information, including name, ABN, or Trademark (TM) number will result in registration, trade, and renewals failures. An ownership change might be required to correct information for existing domains.

Privacy protection

All information is hidden except the name of the registrant contact.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Between 60 days before expiration and the expiration date

- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 29 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 30 days after expiration

Registrar

Our registrar associate, Gandi, uses DomainDirectors as the registrar for this TLD.

Deletion of domain registration

The registry for .au domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

Changing ownership

Change the owner by using the Route 53 console. See [Updating contact information for a domain \(p. 54\)](#). Then complete the following process to complete the ownership change:

1. Both the old and new registrants must click the link they receive in an email from *noreply@emailverification.info* to their listed email addresses. If this isn't completed within 14 days, you have to start the process again.
2. After the responses are confirmed, the owner change in the registry will be processed in a short time without any further confirmation.

FAQ for .au domains

When will I be able to register .au domains?

The .au TLD will be available for registration starting 24 March 2022. You can register .au domains through Route 53 console, unless the domain you want to register is reserved as part of the Priority Allocation Process.

For more information, see [Registering a new domain \(p. 42\)](#).

How do I register .au Domain?

The registration for .au domain will be same as other domains as long as the domain you want to register isn't reserved as part of the Priority Allocation Process.

What are the requirements for registering .au domain?

For the general requirements of .au registration, see [.au direct](#) by auDA.

How can I check if I am able to participate in the Priority Allocation Process?

You can check the priorities and the status for your domain name by using the [priority status tool](#) provided by auDA.

How can I participate in the Priority Allocation Process?

To participate in the Priority Allocation Process, you will need to register your .au domain as you would other domains. We will process the Priority Allocation automatically if the domain and contact information you apply with is eligible for it. Due to the Priority Allocation Process your domain registration can end up in pending-status. For more information, see [the Priority Allocation Process](#).

Otherwise, the domain can be registered directly. Make sure the contact information for your existing domain is up-to-date. Stale or invalid contact information can lead to delays processing your application.

Do I need to register .au domain on 24 March 2022 to be able to participate in the Priority Allocation Process?

No. When .au domain launches on 24 March 2022, registrants of eligible .au domain names (such as .com.au and .net.au) have until 20 September 2022 to indicate whether they intend to apply for the exact match of their names in .au domain via the Priority Allocation Process. Participating in the Priority Allocation Process earlier doesn't mean you have priority over other participants. For more information, see [the Priority Allocation Process](#).

Do I need to participate in the Priority Allocation Process if I own a second level .au domain?

No. If you don't want to apply for a .au direct domain for your equivalent second-level .au domain, there is no action required. Your existing domains will not be affected.

Can I still register second-level domain for .au (such as .com.au or .net.au)?

Yes. The original second-level domains will remain in operation. The registration rules for these will not change.

.cc (Cocos (Keeling) Islands)

[Return to index](#)

Also used as a generic TLD, often by organizations with "cc" in their names, such as consulting companies, cloud computing companies, or cycling clubs. The extension is a popular alternative to ".com."

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection (applies to all contact types: person, company, association, and public body)

- **Hidden** – address, phone number, fax number, and email address
- **Not hidden** – contact name and organization name

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 30 days and 60 days after expiration
- Domain is deleted from the registry: 65 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.co.nz (New Zealand)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

You can register the following second-level domains with Route 53: .co.nz, .net.nz, and .org.nz. You can't register .nz (first-level) domains with Route 53 or transfer .nz domains to Route 53.

Open to the public, with some restrictions:

- Individuals must be at least 18.
- Organizations must be registered.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 4 days after expiration
- Domain is deleted from Route 53: 4 days after expiration
- Restoration with the registry is possible: Between 4 days and 94 days after expiration
- Domain is deleted from the registry: 94 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.com.au (Australia)

[Return to index](#)

Confirmation email from the TLD registry

Our registrar associate, Gandi, resells .com.au domains through DomainDirectors. When you transfer a domain name to Route 53, DomainDirectors sends an email to the registrant contact for the domain to verify contact information or to authorize transfer requests.

Registration and renewal period

One to five years.

Restrictions

Only second-level domains are available. Route 53 supports the second-level domains .com.au and .net.au.

Open to the public, with some restrictions:

- The .com.au and .net.au domains are open to partnerships or sole traders registered in Australia; to foreign companies licensed to trade in Australia; and to owners or applicants of an Australian-registered trademark. Individuals cannot register .com.au/.net.au domains. The registrant contact must be a company.
- Your domain name must be identical to your name (as registered with the relevant Australian authorities) or to your trademark (or to the abbreviation or acronym for your trademark).
- The domain name should indicate your activity. For example, it should indicate a product that you sell or a service that you provide.
- During the registration process, you must provide the following information:
 - Your registration type: ABN (Australian Business Number), ACN (Australian Company Number), or TM (Trademark) if the domain name corresponds to your trademark.
 - Your ID number, which can be a Medicare card number, a tax file number (TFN), a state driver's license number, or an Australian Business Number (ABN).
 - Your state or province.
- Incorrect or mismatched contact information, including name, ABN, or Trademark (TM) number will result in registration, trade, and renewals failures. An ownership change might be required to correct information for existing domains.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Between 60 days before expiration and the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 29 days after expiration

- Restoration with the registry is possible: No
- Domain is deleted from the registry: 30 days after expiration

Registrar

Our registrar associate, Gandi, uses DomainDirectors as the registrar for this TLD.

Deletion of domain registration

The registry for .com.au domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

Changing ownership

Change the owner, either programmatically or by using the Route 53 console. See [Updating contact information for a domain \(p. 54\)](#). Then complete the following process to complete the ownership change:

1. Both the old and new registrants must click the link they receive in an email from noreply@emailverification.info to their listed email addresses. If this isn't completed within 14 days, you have to start the process again.
2. After the responses are confirmed, the owner change in the registry will be processed in a short time without any further confirmation.

.com.sg (Republic of Singapore)

Important

You can no longer use Route 53 to register new .com.sg domains or transfer .com.sg domains to Route 53. We'll continue to support .com.sg domains that are already registered with Route 53.

[Return to index](#)

Renewal period

One or two years.

Deletion of domain registration

The registry for .com.sg domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .com.sg domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration

- Restoration with the registry is possible: Between 30 days and 60 days after expiration
- Domain is deleted from the registry: 60 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.fm (Federated States of Micronesia)

Also used as a generic TLD, often by organizations involved in online media and broadcasting.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection (applies to all contact types: person, company, association, and public body)

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 44 days after expiration
- Restoration with the registry is possible: Between 44 days and 79 days after expiration
- Domain is deleted from the registry: 84 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.in (India)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: Between 30 days and 60 days after expiration
- Domain is deleted from the registry: 65 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.jp (Japan)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Open to the public, with one restriction:

- Only individuals or companies in Japan can register a .jp domain name.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported for Japanese.

Authorization code not required for transfer to Route 53

If you're transferring a .jp domain to Route 53, you don't need to get an authorization code. Instead, initiate the transfer either programmatically or by using the Route 53 console (see [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#)), and then follow the procedure set by your

current domain registrar. If they ask you for value of the AGNT code for your new registrar, provide them **AGNT-1744**, all uppercase.

Authorization code required for transfer from Route 53

If you're transferring a .jp domain from Route 53 to another registrar, initiate the transfer at your new registrar. There is no need for an auth code at this point. You will receive a confirmation email from address *noreply@gandi.net* that will ask you to choose a link to confirm or reject the transfer. To confirm the transfer, retrieve an auth code for your domain by using Route 53 console or API, then choose the link in the email, and provide the code. For more information, see [Transferring a domain from Amazon Route 53 to another registrar \(p. 83\)](#).

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Between 30 days and 6 days before the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: 6 days before expiration
- Restoration with the registry is possible: Contact [AWS Support](#).
- Domain is deleted from the registry: Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Note

Registering non-general-purpose JP domains such as .co.jp and .or.jp is currently not possible.

.io (British Indian Ocean Territory)

Also used as a generic TLD, often by computer-related organizations such as online services, browser-based games, and startup companies.

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

All information is hidden except state/province and country.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

The registry for .io domains also uses the authorization code as a single-use password for some operations, such as enabling or disabling privacy protection. If you want to perform more than

one operation that requires a password, you must generate another authorization code for each operation.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.net.au (Australia)

[Return to index](#)

Confirmation email from the TLD registry

Our registrar associate, Gandi, resells .net.au domains through DomainDirectors. When you transfer a domain name to Route 53, DomainDirectors sends an email to the registrant contact for the domain to verify contact information or to authorize transfer requests.

Registration and renewal period

One to five years.

Restrictions

Only second-level domains are available. Route 53 supports the second-level domains .com.au and net.au.

Open to the public, with some restrictions:

- The .com.au and .net.au domains are open to legal persons, trading, partnerships, or sole traders registered in Australia; to foreign companies licensed to trade in Australia; and to owners or applicants of an Australian-registered trademark.
- Your domain name must be identical to your name, as registered with the relevant Australian authorities or to your trademark (or to the abbreviation or acronym).
- The domain name should indicate your activity. For example, it should indicate a product that you sell or a service that you provide.
- During the registration process, you must indicate the following:
 - Your registration type: ABN (Australian Business Number), ACN (Australian Company Number), or TM (Trademark) if the domain name corresponds to your trademark.
 - Your ID number, which can be a Medicare card number, a tax file number (TFN), a state driver's license number, or an Australian Business Number (ABN).
 - Your state or province.
- Incorrect or mismatched contact information, including name, ABN, or Trademark (TM) number will result in registration, trade, and renewals failures. An ownership change might be required to correct information for existing domains.

Privacy protection

All information is hidden except the name of the registrant contact.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Between 60 days before expiration and the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 29 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 30 days after expiration

Registrar

Our registrar associate, Gandi, uses DomainDirectors as the registrar for this TLD.

Deletion of domain registration

The registry for .net.au domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

Changing ownership

Change the owner, either programmatically or by using the Route 53 console. See [Updating contact information for a domain \(p. 54\)](#). Then complete the following process to complete the ownership change:

1. Both the old and new registrants must click the link they receive in an email from noreply@emailverification.info to their listed email addresses. If this isn't completed within 14 days, you have to start the process again.
2. After the responses are confirmed, the owner change in the registry will be processed in a short time without any further confirmation.

.net.nz (New Zealand)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Your can register the following second-level domains with Route 53: .co.nz, .net.nz, and .org.nz. You can't register .nz (first-level) domains with Route 53 or transfer .nz domains to Route 53.

Open to the public, with some restrictions:

- Individuals must be at least 18.
- Organizations must be registered.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 4 days after expiration
- Domain is deleted from Route 53: 4 days after expiration
- Restoration with the registry is possible: Between 4 days and 94 days after expiration
- Domain is deleted from the registry: 94 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.org.nz (New Zealand)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Your can register the following second-level domains with Route 53: .co.nz, .net.nz, and .org.nz. You can't register .nz (first-level) domains with Route 53 or transfer .nz domains to Route 53.

Open to the public, with some restrictions:

- Individuals must be at least 18.
- Organizations must be registered.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also

restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 4 days after expiration
- Domain is deleted from Route 53: 4 days after expiration
- Restoration with the registry is possible: Between 4 days and 94 days after expiration
- Domain is deleted from the registry: 94 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

[.qa \(Qatar\)](#)

Important

You can no longer use Route 53 to register new .qa domains or transfer .qa domains to Route 53. We'll continue to support .qa domains that are already registered with Route 53.

[Return to index](#)

Renewal period

One to five years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .qa domains to Route 53.

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration

- Restoration with the registry is possible: No
- Domain is deleted from the registry: 31 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.ru (Russian Federation)

Important

You can no longer use Route 53 to register new .ru domains or transfer .ru domains to Route 53. We'll continue to support .ru domains that are already registered with Route 53.

[Return to index](#)

Registration and renewal period

One year.

Note

The registry for .ru domains updates the expiration date for a domain on the day that the domain expires. WHOIS queries will show the old expiration date for the domain until that date regardless of when you renew the domain with Route 53.

Restrictions

Open to the public, with some restrictions:

- Individuals might need to provide a passport number or government-issued ID number.
- Foreign companies might need to provide a company ID or company registration.

Privacy protection

Determined by the registry.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .ru domains to Route 53.

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until 2 days before the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: 2 days before expiration
- Restoration with the registry is possible: Between 2 days before and 28 days after expiration
- Domain is deleted from the registry: 28 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .ru domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

.sg (Republic of Singapore)

Important

You can no longer use Route 53 to register new .sg domains or transfer .sg domains to Route 53. We'll continue to support .sg domains that are already registered with Route 53.

[Return to index](#)

Renewal period

One or two years.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Authorization code required for transfer to Route 53

Not supported. You can no longer transfer .sg domains to Route 53.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: Between 30 days and 60 days after expiration
- Domain is deleted from the registry: 60 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .sg domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

Europe

You can use the following top-level domains (TLDs) for Europe to register domains with Amazon Route 53.

the section called ".be (Belgium)", the section called ".berlin (city of Berlin in Germany)", the section called ".ch (Switzerland)", the section called ".co.uk (United Kingdom)", the section called ".cz (Czech Republic)", the section called ".de (Germany)", the section called ".es (Spain)", the section called ".eu (European Union)", the section called ".fi (Finland)", the section called ".fr (France)", the section called ".gg (Guernsey)", the section called ".im (Isle of Man)", the section called ".it (Italy)", the section

called ".me (Montenegro)", the section called ".me.uk (United Kingdom)", the section called ".nl (the Netherlands)", the section called ".org.uk (United Kingdom)", the section called ".ruhr (Ruhr region, western part of Germany)", the section called ".se (Sweden)", the section called ".uk (United Kingdom)", the section called ".wien (city of Vienna in Austria)"

[Return to index](#)

.be (Belgium)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: On the expiration date
- Restoration with the registry is possible: Until 40 days after expiration
- Domain is deleted from the registry: 40 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.berlin (city of Berlin in Germany)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with some restrictions:

- The owner, administrative, or technical contact must provide an address in Berlin, and the administrative contact must be an individual.

- You must activate and use your .berlin domain within 12 months following its registration (applies to a website, redirection, or email address).
- If you publish a website under your .berlin domain, or if your .berlin domain redirects to another website, the content of the website must be related to Berlin.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Latin and Cyrillic.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.ch (Switzerland)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 9 days after expiration
- Domain is deleted from Route 53: 9 days after expiration
- Restoration with the registry is possible: Between 9 days and 49 days after expiration
- Domain is deleted from the registry: 49 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.co.uk (United Kingdom)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

If you're transferring a .co.uk domain to Route 53, you don't need to get an authorization code. Instead, use the method provided by your current domain registrar to update the value of the IPS tag for the domain to **GANDI**, all uppercase. (An IPS tag is required by Nominet, the registry for .uk domain names.) If your registrar will not change the value of the IPS tag, [contact Nominet](#).

Note

When you register a .co.uk domain, Route 53 automatically sets the IPS tag for the domain to **GANDI**.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Between 180 days before and 30 days after the expiration date
- Late renewal with Route 53 is possible: Between 30 days and 90 days after expiration

- Domain is deleted from Route 53: 90 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 92 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .co.uk domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

.cz (Czech Republic)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported, but email address and phone number are hidden for all contacts.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 58 days after expiration
- Domain is deleted from Route 53: 59 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 60 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.de (Germany)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Open to the public, with some restrictions:

- You must reside in Germany or have an administrative contact (physical person) who resides in Germany and has an address other than a P.O. box.
- During registration, the DNS (A, MX, and CNAME) of the domain name must be correctly configured so that it can pass the registry's zone check. Three servers of two different C classes are required.
- If you're using a DNS service other than Route 53, the name servers for the domain must pass a check to ensure that they're correctly configured. To determine whether the name servers for your domain will pass the check, see <https://www.denic.de/en/service/tools/nast/>.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: On the expiration date
- Restoration with the registry is possible: Contact [AWS Support](#).
- Domain is deleted from the registry: Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.es (Spain)

[Return to index](#)

Domain purchase or transfer

Important

You currently can purchase new .es domain names or transfer .es domains to Route 53 if the contact type for the registrant contact is **Person**. You can't purchase or transfer .es domains if the contact type for the registrant contact is **Company**, **Association**, or **Public Body**.

Registration and renewal period

One to five years.

Restrictions

Open to the public, for those who have an interest in or connection with Spain.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

No

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until 6 days before the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: 6 days before expiration
- Restoration with the registry is possible: Between 6 days before and 4 days after expiration
- Domain is deleted from the registry: 4 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.eu (European Union)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with one restriction:

- You must provide a valid postal address from one of the 30 states of the European Economic Area (EEA) or if you're a citizen of one of the 27 member-states of the European Union (EU), you must specify your EU country of citizenship.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other

programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: On the expiration date
- Restoration with the registry is possible: Until 40 days after expiration
- Domain is deleted from the registry: 40 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

WHOIS Search

For information about existing .eu domains, see <https://whois.eurid.eu/en/>.

[.fi \(Finland\)](#)

[Return to index](#)

Registration and renewal period

One to five years.

Restrictions

Open to the public, with some restrictions:

- The .fi extension is available to individuals who have a domicile in Finland and have a Finnish identity number, and legal persons or private entrepreneurs registered in Finland.
- You must provide the following information during registration:
 - Whether or not the contact is based on a physical or moral person in Finland.
 - The identifier of the register where the name is recorded, if based on a moral person's name.
 - The number of the record in the register where the name is recorded, if based on a moral person's name.
 - The identification number for a moral person in Finland.
 - The identification number for a physical person in Finland.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other

programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: No

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

For information about deleting domains, see [Deleting a domain name registration \(p. 93\)](#).

[**.fr \(France\)**](#)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with some restrictions:

- Individuals must be at least 18 and must provide their date-of-birth.
- Organizations must be located in the European Economic Area or in Switzerland.
- Organizations should fill out all company identification fields (VAT number, SIREN, WALDEC, DUNS, and so on), as this will facilitate any verification that AFNIC might perform at a later date.
- The same eligibility conditions apply to the administrative contact.
- Names and terms are subject to an AFNIC prior review (Naming Charter Article 2.4) and to the following additional conditions:
 - Domain names previously reserved or prohibited are open to applicants that justify a legitimate right and act in good faith.
 - Names beginning with ville, mairie, agglo, cc, cg, and cr are subject to AFNIC naming conventions.

Privacy protection

Determined by the registry.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also

restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 27 days after expiration
- Domain is deleted from Route 53: 28 days after expiration
- Restoration with the registry is possible: Between 28 days and 58 days after expiration
- Domain is deleted from the registry: 58 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

[.gg \(Guernsey\)](#)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: Between 30 days and 35 days after expiration

- Domain is deleted from the registry: 35 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.im (Isle of Man)

Also used as a generic TLD, often by instant messaging services or for individuals who want to develop an "I am" personal brand.

[Return to index](#)

Registration and renewal period

One or two years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 30 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.it (Italy)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Open to the public, with some restrictions:

- Individuals or organizations must have a registered address in the European Union.

- If your country of origin is Italy, you must enter a fiscal code. If your country of origin is within the European Union, you must enter an identity document number (ID number).
- If you specify **Company**, **Association**, or **Public body** for the contact type, a VAT number (a value-added tax identification number) is required.
- Name servers for your domain must pass a DNS check. We suggest that you check the name servers at <https://dns-check.nic.it/> before you submit the change request. If your domain name does not comply with the technical requirements (for example, it isn't associated with an operational name server), and you do not correct it within 30 days, your domain name will be deleted by the registry. We don't issue refunds for domains that are deleted because they don't meet technical requirements.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 13 days after expiration
- Domain is deleted from Route 53: 14 days after expiration
- Restoration with the registry is possible: Between 14 days and 44 days after expiration
- Domain is deleted from the registry: Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.me (Montenegro)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Domain.me, the registry for .me domains, considers two-letter domain names and some longer domain names to be premium domain names. You can't register premium .me domains with or transfer them to Route 53. For more information about premium .me domain names, see the [domain.me](#) website.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Arabic, Belarusian, Bosnian, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Danish, French, German, Hindi, Hungarian, Icelandic, Italian, Korean, Latvian, Lithuanian, Mongolian, Montenegrin, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Turkish, and Ukrainian.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 29 days after expiration
- Domain is deleted from Route 53: 30 days after expiration
- Restoration with the registry is possible: Between 30 days and 60 days after expiration
- Domain is deleted from the registry: 65 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.me.uk (United Kingdom)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

If you're transferring a .me.uk domain to Route 53, you don't need to get an authorization code. Instead, use the method provided by your current domain registrar to update the value of the IPS tag for the domain to **GANDI**, all uppercase. (An IPS tag is required by Nominet, the registry for .uk domain names.) If your registrar will not change the value of the IPS tag, [contact Nominet](#).

Note

When you register a .me.uk domain, Route 53 automatically sets the IPS tag for the domain to **GANDI**.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Between 180 days before and 30 days after the expiration date
- Late renewal with Route 53 is possible: Between 30 days and 90 days after expiration
- Domain is deleted from Route 53: 90 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 92 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .me.uk domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

[**.nl \(the Netherlands\)**](#)

[Return to index](#)

Registration and renewal period

One year.

Restrictions

Open to the public, with some restrictions:

- The owner or the administrative contact must provide a valid address in the Netherlands. A local presence is required.
- If you do not have a valid address in the Netherlands, the Registry SIDN will provide you with a domicile address, as per the Domicile Address Procedure.
- The domain name must be 3-63 characters, excluding .nl.

Privacy protection

Determined by the registry.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until 1 day before the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: 1 day before expiration
- Restoration with the registry is possible: Between 1 day before and 39 days after expiration
- Domain is deleted from the registry: 39 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.org.uk (United Kingdom)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

If you're transferring a .org.uk domain to Route 53, you don't need to get an authorization code. Instead, use the method provided by your current domain registrar to update the value of the IPS tag for the domain to **GANDI**, all uppercase. (An IPS tag is required by Nominet, the registry for .uk domain names.) If your registrar will not change the value of the IPS tag, [contact Nominet](#).

Note

When you register a .org.uk domain, Route 53 automatically sets the IPS tag for the domain to **GANDI**.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Between 180 days before and 30 days after the expiration date
- Late renewal with Route 53 is possible: Between 30 days and 90 days after expiration

- Domain is deleted from Route 53: 90 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 92 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .org.uk domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

.ruhr (Ruhr region, western part of Germany)

[Return to index](#)

The .ruhr extension is for the Ruhr region (western part of Germany).

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with one restriction:

- The administrative contact must be an individual who has an address in Germany.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported (ä, ö, ü, ß).

Authorization code required for transfer to Route 53

Yes

DNSSEC

Not supported.

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: Contact [AWS Support](#).

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.se (Sweden)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with some restrictions:

- If you are located in Sweden, you must provide a valid Swedish ID number.
- If you are located outside of Sweden, you must enter a valid ID number such as a tax ID number.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Supported for Latin, Swedish, and Yiddish.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until 1 day before the expiration date
- Late renewal with Route 53 is possible: No
- Domain is deleted from Route 53: 1 day before expiration
- Restoration with the registry is possible: Between 1 day before and 59 days after expiration
- Domain is deleted from the registry: 64 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

.uk (United Kingdom)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with no restrictions.

Privacy protection

All information is hidden.

Domain locking to prevent unauthorized transfers

Not supported. We recommend that you prevent unauthorized transfers by restricting access to the [RetrieveDomainAuthCode](#) API action. (When you restrict access to this Route 53 API, you also

restrict who can generate an authorization code using the Route 53 console, AWS SDKs, and other programmatic methods.) For more information, see [Identity and access management in Amazon Route 53 \(p. 574\)](#).

Internationalized domain names

Not supported.

Authorization code required for transfer to Route 53

If you're transferring a .uk domain to Route 53, you don't need to get an authorization code. Instead, use the method provided by your current domain registrar to update the value of the IPS tag for the domain to **GANDI**, all uppercase. (An IPS tag is required by Nominet, the registry for .uk domain names.) If your registrar will not change the value of the IPS tag, [contact Nominet](#).

Note

When you register a .uk domain, Route 53 automatically sets the IPS tag for the domain to **GANDI**.

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Between 180 days before and 30 days after the expiration date
- Late renewal with Route 53 is possible: Between 30 days and 90 days after expiration
- Domain is deleted from Route 53: 90 days after expiration
- Restoration with the registry is possible: No
- Domain is deleted from the registry: 92 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Deletion of domain registration

The registry for .uk domains doesn't allow you to delete domain registrations. Instead, you must disable automatic renewal and wait for the domain to expire. For more information, see [Deleting a domain name registration \(p. 93\)](#).

.wien (city of Vienna in Austria)

[Return to index](#)

Registration and renewal period

One to ten years.

Restrictions

Open to the public, with some restrictions:

- You must show an economic, cultural, tourist, historical, social, or other affinity with the city of Vienna in Austria.
- The .wien domain names must be used in connection with the above conditions, throughout the term of registration.

Privacy protection

Not supported.

Domain locking to prevent unauthorized transfers

Supported.

Internationalized domain names

Supported for Latin.

Authorization code required for transfer to Route 53

Yes

DNSSEC

Supported for domain registration. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

Deadlines for renewing and restoring domains

- Renewal is possible: Until the expiration date
- Late renewal with Route 53 is possible: Until 44 days after expiration
- Domain is deleted from Route 53: 45 days after expiration
- Restoration with the registry is possible: Between 45 days and 75 days after expiration
- Domain is deleted from the registry: 80 days after expiration

Registrar

The registrar for this TLD is our registrar associate, Gandi.

Configuring Amazon Route 53 as your DNS service

You can use Amazon Route 53 as the DNS service for your domain, such as example.com. When Route 53 is your DNS service, it routes internet traffic to your website by translating friendly domain names like www.example.com into numeric IP addresses, like 192.0.2.1, that computers use to connect to each other. When someone types your domain name in a browser or sends you an email, a DNS query is forwarded to Route 53, which responds with the appropriate value. For example, Route 53 might respond with the IP address for the web server for example.com.

In this chapter, we explain how to configure Route 53 to route your internet traffic to the right places. We also explain how to migrate DNS service to Route 53 if you're currently using another DNS service, and how to use Route 53 as the DNS service for a new domain.

Topics

- [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#)
- [Configuring DNS routing for a new domain \(p. 334\)](#)
- [Routing traffic to your resources \(p. 335\)](#)
- [Working with hosted zones \(p. 339\)](#)
- [Working with records \(p. 370\)](#)
- [Using traffic flow to route DNS traffic \(p. 442\)](#)
- [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#)
- [Using AWS Cloud Map to create records and health checks \(p. 470\)](#)
- [DNS constraints and behaviors \(p. 470\)](#)

Making Amazon Route 53 the DNS service for an existing domain

If you're transferring one or more domain registrations to Route 53, and you're currently using a domain registrar that doesn't provide paid DNS service, you need to migrate DNS service before you migrate the domain. Otherwise, the registrar will stop providing DNS service when you transfer your domains, and the associated websites and web applications will become unavailable on the internet. (You can also migrate DNS service from the current registrar to another DNS service provider. We don't require you to use Route 53 as the DNS service provider for domains that are registered with Route 53.)

The process depends on whether you're currently using the domain:

- If the domain is currently getting traffic—for example, if your users are using the domain name to browse to a website or access a web application—see [Making Route 53 the DNS service for a domain that's in use \(p. 326\)](#).
- If the domain isn't getting any traffic (or is getting very little traffic), see [Making Route 53 the DNS service for an inactive domain \(p. 331\)](#).

For both options, your domain should remain available during the entire migration process. However, in the unlikely event that there are issues, the first option lets you roll back the migration quickly. With the second option, your domain could be unavailable for a couple of days.

Making Route 53 the DNS service for a domain that's in use

If you want to migrate DNS service to Amazon Route 53 for a domain that is currently getting traffic—for example, if your users are using the domain name to browse to a website or access a web application—perform the procedures in this section.

Topics

- [Step 1: Get your current DNS configuration from the current DNS service provider \(optional but recommended\) \(p. 326\)](#)
- [Step 2: Create a hosted zone \(p. 327\)](#)
- [Step 3: Create records \(p. 328\)](#)
- [Step 4: Lower TTL settings \(p. 328\)](#)
- [Step 5: \(If you have DNSSEC configured\) Remove the DS record from the parent zone \(p. 329\)](#)
- [Step 6: Wait for the old TTL to expire \(p. 329\)](#)
- [Step 7: Update the NS records to use Route 53 name servers \(p. 329\)](#)
- [Step 8: Monitor traffic for the domain \(p. 330\)](#)
- [Step 9: Change the TTL for the NS record back to a higher value \(p. 330\)](#)
- [Step 10: Transfer domain registration to Amazon Route 53 \(p. 331\)](#)
- [Step 11: Re-enable DNSSEC signing \(if required\) \(p. 331\)](#)

Step 1: Get your current DNS configuration from the current DNS service provider (optional but recommended)

When you migrate DNS service from another provider to Route 53, you reproduce your current DNS configuration in Route 53. In Route 53, you create a hosted zone that has the same name as your domain, and you create records in the hosted zone. Each record indicates how you want to route traffic for a specified domain name or subdomain name. For example, when someone enters your domain name in a web browser, do you want traffic to be routed to a web server in your data center, to an Amazon EC2 instance, to a CloudFront distribution, or to some other location?

The process that you use depends on the complexity of your current DNS configuration:

- **If your current DNS configuration is simple** – If you're routing internet traffic for just a few subdomains to a small number of resources, such as web servers or Amazon S3 buckets, then you can manually create a few records in the Route 53 console.
- **If your current DNS configuration is more complex, and you just want to reproduce your current configuration** – You can simplify the migration if you can get a zone file from the current DNS service provider, and import the zone file into Route 53. (Not all DNS service providers offer zone files.) When you import a zone file, Route 53 automatically reproduces the existing configuration by creating the corresponding records in your hosted zone.

Try asking customer support with your current DNS service provider how to get a *zone file* or a *records list*. For information about the required format of the zone file, see [Creating records by importing a zone file \(p. 438\)](#).

- **If your current DNS configuration is more complex, and you're interested in Route 53 routing features** – Review the following documentation to see whether you want to use Route 53 features that aren't available from other DNS service providers. If so, you can either create records manually, or you can import a zone file and then create or update records later:

- [Choosing between alias and non-alias records \(p. 379\)](#) explains the advantages of Route 53 alias records, which route traffic to some AWS resources, such as CloudFront distributions and Amazon S3 buckets, for no charge.
- [Choosing a routing policy \(p. 371\)](#) explains the Route 53 routing options, for example, routing based on the location of your users, routing based on the latency between your users and your resources, routing based on whether your resources are healthy, and routing to resources based on weights that you specify.

Note

You can also import a zone file and later change your configuration to take advantage of alias records and complex routing policies.

If you can't get a zone file or if you want to manually create records in Route 53, the records that you're likely to migrate include the following:

- **A (Address) records** – associate a domain name or subdomain name with the IPv4 address (for example, 192.0.2.3) of the corresponding resource
- **AAAA (Address) records** – associate a domain name or subdomain name with the IPv6 address (for example, 2001:0db8:85a3:0000:0000:abcd:0001:2345) of the corresponding resource
- **Mail server (MX) records** – route traffic to mail servers
- **CNAME records** – reroute traffic for one domain name (example.net) to another domain name (example.com)
- **Records for other supported DNS record types** – For a list of supported record types, see [Supported DNS record types \(p. 382\)](#).

Step 2: Create a hosted zone

To tell Amazon Route 53 how you want to route traffic for your domain, you create a hosted zone that has the same name as your domain, and then you create records in the hosted zone.

Important

You can create a hosted zone only for a domain that you have permission to administer.

Typically, this means that you own the domain, but you might also be developing an application for the domain registrant.

When you create a hosted zone, Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone. The NS record identifies the four name servers that Route 53 associates with your hosted zone. To make Route 53 the DNS service for your domain, you update the registration for the domain to use these four name servers.

Important

Don't create additional name server (NS) or start of authority (SOA) records, and don't delete the existing NS and SOA records.

To create a hosted zone

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started** under **DNS management**, and then choose **Create hosted zones**.
If you're already using Route 53, choose **Hosted zones** in the navigation pane, and then choose **Create hosted zones**.
3. In the **Create hosted zone** pane, enter a domain name and, optionally, a comment. For more information about a setting, choose to open the help panel on the right side.

For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).

4. For **Type**, accept the default value of **Public hosted zone**.
5. Choose **Create hosted zone**.

Step 3: Create records

After you create a hosted zone, you create records in the hosted zone that define where you want to route traffic for a domain (example.com) or subdomain (www.example.com). For example, if you want to route traffic for example.com and www.example.com to a web server on an Amazon EC2 instance, you create two records, one named example.com and the other named www.example.com. In each record, you specify the IP address for your EC2 instance.

You can create records in a variety of ways:

Import a zone file

This is the easiest method if you got a zone file from your current DNS service in [Step 1: Get your current DNS configuration from the current DNS service provider \(optional but recommended\) \(p. 326\)](#). Amazon Route 53 can't predict when to create alias records or to use special routing types such as weighted or failover. As a result, if you import a zone file, Route 53 creates standard DNS records using the simple routing policy.

For more information, see [Creating records by importing a zone file \(p. 438\)](#).

Create records individually in the console

If you didn't get a zone file and you just want to create a few records with a routing policy of Simple to get started, you can create the records in the Route 53 console. You can create both alias and non-alias records.

For more information, see the following topics:

- [Choosing a routing policy \(p. 371\)](#)
- [Choosing between alias and non-alias records \(p. 379\)](#)
- [Creating records by using the Amazon Route 53 console \(p. 392\)](#)

Create records programmatically

You can create records by using one of the AWS SDKs, the AWS CLI, or AWS Tools for Windows PowerShell. For more information, see [AWS Documentation](#).

If you're using a programming language that AWS doesn't provide an SDK for, you can also use the Route 53 API. For more information, see the [Amazon Route 53 API Reference](#).

Step 4: Lower TTL settings

The TTL (time to live) setting for a record specifies how long you want DNS resolvers to cache the record and use the cached information. When the TTL expires, a resolver sends another query to the DNS service provider for a domain to get the latest information.

The typical TTL setting for the NS record is 172800 seconds, or two days. The NS record lists the name servers that the Domain Name System (DNS) can use to get information about how to route traffic for your domain. Lowering the TTL for the NS record, both with your current DNS service provider and with Amazon Route 53, reduces downtime for your domain if you discover a problem while you're migrating DNS to Route 53. If you don't lower the TTL, your domain could be unavailable on the internet for up to two days if something goes wrong.

We recommend that you change the TTL on the following NS records:

- On the NS record in the hosted zone for the current DNS service provider. (Your current provider might use different terminology.)
- On the NS record in the hosted zone that you created in [Step 2: Create a hosted zone \(p. 327\)](#).

To lower the TTL setting on the NS record with the current DNS service provider

- Use the method provided by the current DNS service provider for the domain to change the TTL for the NS record in the hosted zone for your domain.

To lower the TTL setting on the NS record in a Route 53 hosted zone

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Choose **Hosted Zones** in the navigation pane.
3. Choose the name of the hosted zone.
4. Choose the NS record, and choose **Edit**.
5. Change the value of **TTL (Seconds)**. We recommend that you specify a value between 60 seconds and 900 seconds (15 minutes).
6. Choose **Save changes**.

Step 5: (If you have DNSSEC configured) Remove the DS record from the parent zone

If you've configured DNSSEC for your domain, remove the Delegation Signer (DS) record from the parent zone before you migrate your domain to Route 53.

Because it isn't currently possible to have DNSSEC signing enabled across two providers, you must remove any DS or DNSKEYs to deactivate DNSSEC. This temporarily signals to DNS resolvers to disable DNSSEC validation. In [step 11 \(p. 331\)](#), you can re-enable DNSSEC validation if desired, after the transition to Route 53 is completed.

For more information, see [Deleting public keys for a domain \(p. 92\)](#).

Step 6: Wait for the old TTL to expire

If your domain is in use—for example, if your users are using the domain name to browse to a website or access a web application—then DNS resolvers have cached the names of the name servers that were provided by your current DNS service provider. A DNS resolver that cached that information a few minutes ago will save it for almost two more days.

To ensure that migrating DNS service to Route 53 happens all at one time, wait for two days after you lowered the TTL. After the two-day TTL expires and resolvers request the name servers for your domain, the resolvers will get the current name servers and will also get the new TTL that you specified in [Step 4: Lower TTL settings \(p. 328\)](#).

Step 7: Update the NS records to use Route 53 name servers

To begin using Amazon Route 53 as the DNS service for a domain, use the method provided by the registrar, or the parent zone, to replace the current name servers in the NS record with Route 53 name servers.

Note

When you update the NS record with the current DNS service provider to use Route 53 name servers, you're updating the DNS configuration for the domain. (This is comparable to updating the NS record in the Route 53 hosted zone for a domain except that you're updating the setting with the DNS service that you're migrating away from.)

To update the NS record at the registrar, or the parent zone, to use Route 53 name servers

1. In the Route 53 console, get the name servers for your hosted zone:
 - a. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 - b. In the navigation pane, choose **Hosted zones**.
 - c. On the **Hosted zones** page, choose the name for the applicable hosted zone.
 - d. Make note of the four names listed for **Name servers** in the **Hosted zone details** section.
2. Use the method that is provided by the current DNS service for the domain to update the NS record for the hosted zone. If the domain is registered with Route 53, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#). The process depends on whether the current DNS service lets you delete name servers:

If you can delete name servers

- Make note of the names of the current name servers in the NS record for the hosted zone. If you need to revert to the current DNS configuration, these are the servers that you'll specify.
- Delete the current name servers from the NS record.
- Update the NS record with the names of all four of the Route 53 name servers that you got in step 1 of this procedure.

Note

When you're finished, the only name servers in the NS record will be the four Route 53 name servers.

If you cannot delete name servers

- Choose the option to use custom name servers.
- Add all four Route 53 name servers that you got in step 1 of this procedure.

Step 8: Monitor traffic for the domain

Monitor traffic for the domain, including website or application traffic, and email:

- **If the traffic slows or stops** – Use the method provided by the previous DNS service to change the name servers for the domain back to the previous name servers. These are the name servers that you made note of in step 7 of [To update the NS record at the registrar, or the parent zone, to use Route 53 name servers \(p. 330\)](#). Then determine what went wrong.
- **If the traffic is unaffected** – Continue to [Step 9: Change the TTL for the NS record back to a higher value \(p. 330\)](#).

Step 9: Change the TTL for the NS record back to a higher value

In the Amazon Route 53 hosted zone for the domain, change the TTL for the NS record to a more typical value, for example, 172800 seconds (two days). This improves latency for your users because they don't have to wait as often for DNS resolvers to send a query for the name servers for your domain.

To change the TTL for the NS record in the Route 53 hosted zone

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Choose **Hosted Zones** in the navigation pane.
3. Choose the name of the hosted zone.
4. In the list of records for the hosted zone, choose the NS record.
5. Choose **Edit**.
6. Change **TTL (Seconds)** to the number of seconds that you want DNS resolvers to cache the names of the name servers for your domain. We recommend a value of 172800 seconds.
7. Choose **Save changes**.

Step 10: Transfer domain registration to Amazon Route 53

Now that you've transferred DNS service for a domain to Amazon Route 53, you can optionally transfer registration for the domain to Route 53. For more information, see [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#).

Step 11: Re-enable DNSSEC signing (if required)

Now that you've transferred DNS service for a domain to Amazon Route 53, you can re-enable DNSSEC signing.

Enabling DNSSEC signing has two steps:

- Step 1: Enable DNSSEC signing for Route 53, and request that Route 53 create a key signing key (KSK) based on a customer managed key in AWS Key Management Service (AWS KMS).
- Step 2: Create a chain of trust for the hosted zone by adding a Delegation Signer (DS) record to the parent zone, so DNS responses can be authenticated with trusted cryptographic signatures.

For instructions, see [Enabling DNSSEC signing and establishing a chain of trust \(p. 456\)](#).

Making Route 53 the DNS service for an inactive domain

If you want to migrate DNS service to Amazon Route 53 for a domain that isn't getting any traffic (or is getting very little traffic), perform the procedures in this section.

Topics

- [Step 1: Get your current DNS configuration from the current DNS service provider \(inactive domains\) \(p. 332\)](#)
- [Step 2: Create a hosted zone \(inactive domains\) \(p. 333\)](#)
- [Step 3: Create records \(inactive domains\) \(p. 333\)](#)
- [Step 4: Update the domain registration to use Amazon Route 53 name servers \(inactive domains\) \(p. 334\)](#)

Step 1: Get your current DNS configuration from the current DNS service provider (inactive domains)

When you migrate DNS service from another provider to Route 53, you reproduce your current DNS configuration in Route 53. In Route 53, you create a hosted zone that has the same name as your domain, and you create records in the hosted zone. Each record indicates how you want to route traffic for a specified domain name or subdomain name. For example, when someone enters your domain name in a web browser, do you want traffic to be routed to a web server in your data center, to an Amazon EC2 instance, to a CloudFront distribution, or to some other location?

The process that you use depends on the complexity of your current DNS configuration:

- **If your current DNS configuration is simple** – If you're routing internet traffic for just a few subdomains to a small number of resources, such as web servers or Amazon S3 buckets, then you can manually create a few records in the Route 53 console.
- **If your current DNS configuration is more complex, and you just want to reproduce your current configuration** – You can simplify the migration if you can get a zone file from the current DNS service provider, and import the zone file into Route 53. (Not all DNS service providers offer zone files.) When you import a zone file, Route 53 automatically reproduces the existing configuration by creating the corresponding records in your hosted zone.

Try asking customer support with your current DNS service provider how to get a *zone file* or a *records list*. For information about the required format of the zone file, see [Creating records by importing a zone file \(p. 438\)](#).

- **If your current DNS configuration is more complex, and you're interested in Route 53 routing features** – Review the following documentation to see whether you want to use Route 53 features that aren't available from other DNS service providers. If so, you can either create records manually, or you can import a zone file and then create or update records later:
 - [Choosing between alias and non-alias records \(p. 379\)](#) explains the advantages of Route 53 alias records, which route traffic to some AWS resources, such as CloudFront distributions and Amazon S3 buckets, for no charge.
 - [Choosing a routing policy \(p. 371\)](#) explains the Route 53 routing options, for example, routing based on the location of your users, routing based on the latency between your users and your resources, routing based on whether your resources are healthy, and routing to resources based on weights that you specify.

Note

You can also import a zone file and later change your configuration to take advantage of alias records and complex routing policies.

If you can't get a zone file or if you want to manually create records in Route 53, the records that you're likely to migrate include the following:

- **A (Address) records** – associate a domain name or subdomain name with the IPv4 address (for example, 192.0.2.3) of the corresponding resource
- **AAAA (Address) records** – associate a domain name or subdomain name with the IPv6 address (for example, 2001:0db8:85a3:0000:0000:abcd:0001:2345) of the corresponding resource
- **Mail server (MX) records** – route traffic to mail servers
- **CNAME records** – reroute traffic for one domain name (example.net) to another domain name (example.com)
- **Records for other supported DNS record types** – For a list of supported record types, see [Supported DNS record types \(p. 382\)](#).

Step 2: Create a hosted zone (inactive domains)

To tell Amazon Route 53 how you want to route traffic for your domain, you create a hosted zone that has the same name as your domain, and then you create records in the hosted zone.

Important

You can create a hosted zone only for a domain that you have permission to administer. Typically, this means that you own the domain, but you might also be developing an application for the domain registrant.

When you create a hosted zone, Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone. The NS record identifies the four name servers that Route 53 associates with your hosted zone. To make Route 53 the DNS service for your domain, you update the registration for the domain to use these four name servers.

Important

Don't create additional name server (NS) or start of authority (SOA) records, and don't delete the existing NS and SOA records.

To create a hosted zone

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started**.
If you're already using Route 53, choose **Hosted zones** in the navigation pane.
3. Choose **Create hosted zone**.
4. In the **Create hosted zone** pane, enter a domain name and, optionally, a comment. For more information about a setting, pause the mouse pointer over its label to see a tool tip.
For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).
5. For **Record type**, accept the default value of **Public hosted zone**.
6. Choose **Create hosted zone**.

Step 3: Create records (inactive domains)

After you create a hosted zone, you create records in the hosted zone that define where you want to route traffic for a domain (example.com) or subdomain (www.example.com). For example, if you want to route traffic for example.com and www.example.com to a web server on an Amazon EC2 instance, you create two records, one named example.com and the other named www.example.com. In each record, you specify the IP address for your EC2 instance.

You can create records in a variety of ways:

Import a zone file

This is the easiest method if you got a zone file from your current DNS service in [Step 1: Get your current DNS configuration from the current DNS service provider \(inactive domains\) \(p. 332\)](#).

Amazon Route 53 can't predict when to create alias records or to use special routing types such as weighted or failover. As a result, if you import a zone file, Route 53 creates standard DNS records using the simple routing policy.

For more information, see [Creating records by importing a zone file \(p. 438\)](#).

Create records individually in the console

If you didn't get a zone file and you just want to create a few records with a routing policy of Simple to get started, you can create the records in the Route 53 console. You can create both alias and non-alias records.

For more information, see the following topics:

- [Choosing a routing policy \(p. 371\)](#)
- [Choosing between alias and non-alias records \(p. 379\)](#)
- [Creating records by using the Amazon Route 53 console \(p. 392\)](#)

Create records programmatically

You can create records by using one of the AWS SDKs, the AWS CLI, or AWS Tools for Windows PowerShell. For more information, see [AWS Documentation](#).

If you're using a programming language that AWS doesn't provide an SDK for, you can also use the Route 53 API. For more information, see the [Amazon Route 53 API Reference](#).

Step 4: Update the domain registration to use Amazon Route 53 name servers (inactive domains)

When you've finished creating records for the domain, you can change the DNS service for your domain to Amazon Route 53. Perform the following procedure to update settings with the domain registrar.

To update the name servers for the domain

1. In the Route 53 console, get the name servers for your Route 53 hosted zone:
 - a. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 - b. In the navigation pane, choose **Hosted zones**.
 - c. On the **Hosted zones** page, choose the radio button (not the name) for the hosted zone, then choose **View details**.
 - d. On the details page for the hosted zone, choose **Hosted zone details**.
 - e. Make note of the four servers listed for **Name servers**.
2. Use the method provided by the registrar for the domain to change the name servers for the domain to use the four Route 53 name servers that you got in step 1 of this procedure.

If the domain is registered with Route 53, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#).

Configuring DNS routing for a new domain

When you register a domain with Route 53, we automatically make Route 53 the DNS service for the domain. Route 53 creates a hosted zone that has the same name as the domain, assigns four name servers to the hosted zone, and updates the domain to use those name servers.

To specify how you want Route 53 to route internet traffic for the domain, you create records in the hosted zone. For example, if you want to route requests for example.com to a web server that's running on an Amazon EC2 instance, you create a record in the example.com hosted zone, and you specify the Elastic IP address for the EC2 instance. For more information, see the following topics:

- For information about how to create records in your hosted zone, see [Working with records \(p. 370\)](#).
- For information about how to route traffic to selected AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

- For information about how DNS works, see [How internet traffic is routed to your website or web application \(p. 2\)](#).

Routing traffic to your resources

When users request your website or web application, for example, by entering the name of your domain in a web browser, Amazon Route 53 helps to route users to your resources, such as an Amazon S3 bucket or a web server in your data center. To configure Route 53 to route traffic to your resources, you do the following:

1. Create a hosted zone. You can create either a public hosted zone or a private hosted zone:

Public hosted zone

Create a public hosted zone if you want to route internet traffic to your resources, for example, so your customers can view the company website that you're hosting on EC2 instances. For more information, see [Working with public hosted zones \(p. 339\)](#).

Private hosted zone

Create a private hosted zone if you want to route traffic within an Amazon VPC. For more information, see [Working with private hosted zones \(p. 356\)](#).

2. Create records in the hosted zone. Records define where you want to route traffic for each domain name or subdomain name. For example, to route traffic for www.example.com to a web server in your data center, you typically create a www.example.com record in the example.com hosted zone.

For more information, see the following topics:

- [Working with records \(p. 370\)](#)
- [Routing traffic for subdomains \(p. 335\)](#)
- [Routing internet traffic to your AWS resources \(p. 496\)](#)

Routing traffic for subdomains

When you want to route traffic to your resources for a subdomain, such as acme.example.com or zenith.example.com, you have two options:

Create records in the hosted zone for the domain

Typically, to route traffic for a subdomain, you create a record in the hosted zone that has the same name as the domain. For example, to route internet traffic for acme.example.com to a web server in your data center, you create a record named acme.example.com in the example.com hosted zone.

For more information, see the topic [Working with records \(p. 370\)](#) and its subtopics.

Create a hosted zone for the subdomain, and create records in the new hosted zone

You can also create a hosted zone for the subdomain. Using a separate hosted zone to route internet traffic for a subdomain is sometimes known as "delegating responsibility for a subdomain to a hosted zone" or "delegating a subdomain to other name servers" or some similar combination of terms. Here's an overview of how it works:

1. You create a hosted zone that has the same name as the subdomain that you want to route traffic for, such as acme.example.com.
2. You create records in the new hosted zone that define how you want to route traffic for the subdomain (acme.example.com) and its subdomains, such as backend.acme.example.com.
3. You get the name servers that Route 53 assigned to the new hosted zone when you created it.
4. You create a new NS record in the hosted zone for the domain (example.com), and you specify the four name servers that you got in step 3.

When you use a separate hosted zone to route traffic for a subdomain, you can use IAM permissions to restrict access to the hosted zone for the subdomain. (You can't use IAM to control access to individual records.) If you have multiple subdomains that are managed by different groups, creating a hosted zone for each subdomain can significantly reduce the number of people who must have access to records in the hosted zone for the domain.

Using a separate hosted zone for a subdomain also allows you to use different DNS services for the domain and the subdomain. For more information, see [Using Amazon Route 53 as the DNS service for subdomains without migrating the parent domain \(p. 656\)](#).

There's a small performance impact to this configuration for the first DNS query from each DNS resolver. The resolver must get information from the hosted zone for the root domain and then get information from the hosted zone for the subdomain. After the first DNS query for a subdomain, the resolver caches the information and doesn't need to get it again until the TTL expires and another client requests the subdomain from that resolver. For more information, see [TTL \(seconds\) \(p. 403\)](#) in the section [Values that you specify when you create or edit Amazon Route 53 records \(p. 393\)](#).

Topics

- [Creating another hosted zone to route traffic for a subdomain \(p. 336\)](#)
- [Routing traffic for additional levels of subdomains \(p. 338\)](#)

Creating another hosted zone to route traffic for a subdomain

One way to route traffic for a subdomain is to create a hosted zone for the subdomain, and then create records for the subdomain in the new hosted zone. (The more common option is to create records for the subdomain in the hosted zone for the domain.)

Note

While we describe here the process for creating and delegating to a subdomain hosted zone on Route 53, you can also create a DNS zone on other name servers and similarly create name server (NS) records that delegate responsibility to those name servers.

Here's an overview of the process:

1. Create a hosted zone for the subdomain. For more information, see [Creating a new hosted zone for a subdomain \(p. 336\)](#).
2. Add records to the hosted zone for the subdomain. If the hosted zone for the domain contains any records that belong in the hosted zone for the subdomain, duplicate those records in the hosted zone for the subdomain. For more information, see [Creating records in the hosted zone for the subdomain \(p. 337\)](#).
3. Create an NS record for the subdomain in the hosted zone for the domain, which delegates responsibility for the subdomain to the name servers in the new hosted zone. If the hosted zone for the domain contains any records that belong in the hosted zone for the subdomain, delete the records from the hosted zone for the domain. (You created copies in the hosted zone for the subdomain in step 2.) For more information, see [Updating the hosted zone for the domain \(p. 337\)](#).

Creating a new hosted zone for a subdomain

To create a hosted zone for a subdomain using the Route 53 console, perform the following procedure.

To create a hosted zone for a subdomain (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started**.

If you're already using Route 53, choose **Hosted zones** in the navigation pane.

3. Choose **Create hosted zone**.
4. In the right pane, enter the name of the subdomain, such as acme.example.com. You can also optionally enter a comment.

For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).

5. For **Type**, accept the default value of **Public hosted zone**.
6. At the bottom of the right pane, choose **Create hosted zone**.

Creating records in the hosted zone for the subdomain

To define how you want Route 53 to route traffic for the subdomain (acme.example.com) and its subdomains (backend.acme.example.com), you create records in the hosted zone for the subdomain.

Note the following about creating records in the hosted zone for the subdomain:

- Don't create additional name server (NS) or start of authority (SOA) records in the hosted zone for the subdomain, and don't delete the existing NS and SOA records.
- Create all records for the subdomain in the hosted zone for the subdomain. For example, if you have hosted zones for example.com and for acme.example.com domain, create all records for the acme.example.com subdomain in the acme.example.com hosted zone. This includes records such as backend.acme.example.com and beta.backend.acme.example.com.
- If the hosted zone for the domain (example.com) already contains records that belong in the hosted zone for the subdomain (acme.example.com), duplicate those records in the hosted zone for the subdomain. In the last step of the process, you delete the duplicate records from the hosted zone for the domain later.

Important

If you have some records for the subdomain in both the hosted zone for the domain and the hosted zone for the subdomain, DNS behavior will be inconsistent. Behavior will depend on which name servers a DNS resolver has cached, the name servers for the domain hosted zone (example.com) or the name servers for the subdomain hosted zone (acme.example.com). In some cases, Route 53 will return NXDOMAIN (non-existent domain) when the record exists, but not in the hosted zone that DNS resolvers are submitting the query to.

For more information, see [Working with records \(p. 370\)](#).

Updating the hosted zone for the domain

When you create a hosted zone, Route 53 automatically assigns four name servers to the zone. The NS record for a hosted zone identifies the name servers that respond to DNS queries for the domain or subdomain. To start using the records in the hosted zone for the subdomain to route internet traffic, you create a new NS record in the hosted zone for the domain (example.com), and give it the name of the subdomain (acme.example.com). For the value of the NS record, you specify the names of the name servers from the hosted zone for the subdomain.

Here's what happens when Route 53 receives a DNS query from a DNS resolver for the subdomain acme.example.com or one of its subdomains:

1. Route 53 looks in the hosted zone for the domain (example.com) and finds the NS record for the subdomain (acme.example.com).
2. Route 53 gets the name servers from the acme.example.com NS record in the hosted zone for the domain, example.com, and returns those name servers to the DNS resolver.

3. The resolver resubmits the query for acme.example.com to the name servers for the acme.example.com hosted zone.
4. Route 53 responds to the query using a record in the acme.example.com hosted zone.

To configure Route 53 to route traffic for the subdomain using the hosted zone for the subdomain and to delete any duplicate records from the hosted zone for the domain, perform the following procedure:

To configure Route 53 to use the hosted zone for the subdomain (console)

1. In the Route 53 console, get the name servers for the hosted zone for the subdomain:
 - a. In the navigation pane, choose **Hosted zones**.
 - b. On the **Hosted zones** page, choose the name for the hosted zone for the subdomain.
 - c. In the right pane, copy the names of the four servers listed for **Name servers** in the **Hosted zones details** section.
2. Choose the name of the hosted zone for the domain (example.com), not for the subdomain.
3. Choose **Create record**.
4. Choose **Simple routing** and choose **Next**.
5. Choose **Define simple record**.
6. Specify the following values:

Name

Enter the name of the subdomain.

Value/Route traffic to

Choose **IP address or another value depending on the record type**, and paste the names of the name servers that you copied in step 1.

Record type

Choose **NS – Name servers for a hosted zone**.

TTL (Seconds)

Change to a more common value for an NS record, such as 172800 seconds.

7. Choose **Define simple record**, and choose **Create records**.
8. If the hosted zone for the domain contains any records that you recreated in the hosted zone for the subdomain, delete those records from the hosted zone for the domain. For more information, see [Deleting records \(p. 440\)](#).

When you're finished, all records for the subdomain should be in the hosted zone for the subdomain.

Routing traffic for additional levels of subdomains

You route traffic to a subdomain of a subdomain, such as backend.acme.example.com, the same way that you route traffic to a subdomain, such as acme.example.com. Either you create records in the hosted zone for the domain, or you create a hosted zone for the lower-level subdomain, and then you create records in that new hosted zone.

If you choose to create a separate hosted zone for the lower-level subdomain, create the NS record for the lower-level subdomain in the hosted zone for the subdomain that is one level closer to the domain name. This helps to ensure that traffic is correctly routed to your resources. For example, suppose you want to route traffic for the following subdomains:

- subdomain1.example.com

- subdomain2.subdomain1.example.com

To use another hosted zone to route traffic for subdomain2.subdomain1.example.com, you do the following:

1. Create a hosted zone named subdomain2.subdomain1.example.com.
2. Create records in the subdomain2.subdomain1.example.com hosted zone. For more information, see [Creating records in the hosted zone for the subdomain \(p. 337\)](#).
3. Copy the names of the name servers for the subdomain2.subdomain1.example.com hosted zone.
4. In the subdomain1.example.com hosted zone, create an NS record named subdomain2.subdomain1.example.com, and paste in the names of the name servers for the subdomain2.subdomain1.example.com hosted zone.

In addition, delete any duplicate records from the subdomain1.example.com. For more information, see [Updating the hosted zone for the domain \(p. 337\)](#).

After you create this NS record, Route 53 starts to use the subdomain2.subdomain1.example.com hosted zone to route traffic for the subdomain2.subdomain1.example.com subdomain.

Working with hosted zones

A hosted zone is a container for records, and records contain information about how you want to route traffic for a specific domain, such as example.com, and its subdomains (acme.example.com, zenith.example.com). A hosted zone and the corresponding domain have the same name. There are two types of hosted zones:

- *Public hosted zones* contain records that specify how you want to route traffic on the internet. For more information, see [Working with public hosted zones \(p. 339\)](#).
- *Private hosted zones* contain records that specify how you want to route traffic in an Amazon VPC. For more information, see [Working with private hosted zones \(p. 356\)](#).

Working with public hosted zones

A public hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain, such as example.com, and its subdomains (acme.example.com, zenith.example.com). You get a public hosted zone in one of two ways:

- When you register a domain with Route 53, we create a hosted zone for you automatically.
- When you transfer DNS service for an existing domain to Route 53, you start by creating a hosted zone for the domain. For more information, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

In both cases, you then create records in the hosted zone to specify how you want to route traffic for the domain and subdomains. For example, you might create a record to route traffic for www.example.com to a CloudFront distribution or to a web server in your data center. For more information about records, see [Working with records \(p. 370\)](#).

This topic explains how to use the Amazon Route 53 console to create, list, and delete public hosted zones.

Note

You can also use a Route 53 *private* hosted zone to route traffic within one or more VPCs that you create with the Amazon VPC service. For more information, see [Working with private hosted zones \(p. 356\)](#).

Topics

- [Considerations when working with public hosted zones \(p. 340\)](#)
- [Creating a public hosted zone \(p. 340\)](#)
- [Getting the name servers for a public hosted zone \(p. 341\)](#)
- [Listing public hosted zones \(p. 342\)](#)
- [Viewing DNS query metrics for a public hosted zone \(p. 342\)](#)
- [Deleting a public hosted zone \(p. 345\)](#)
- [Checking DNS responses from Route 53 \(p. 347\)](#)
- [Configuring white-label name servers \(p. 349\)](#)
- [NS and SOA records that Amazon Route 53 creates for a public hosted zone \(p. 354\)](#)

Considerations when working with public hosted zones

Note the following considerations when working with public hosted zones:

NS and SOA records

When you create a hosted zone, Amazon Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone. The NS record identifies the four name servers that you give to your registrar or your DNS service so that DNS queries are routed to Route 53 name servers. For more information about NS and SOA records, see [NS and SOA records that Amazon Route 53 creates for a public hosted zone \(p. 354\)](#).

Multiple hosted zones that have the same name

You can create more than one hosted zone that has the same name and add different records to each hosted zone. Route 53 assigns four name servers to every hosted zone, and the name servers are different for each of them. When you update your registrar's name server records, be careful to use the Route 53 name servers for the correct hosted zone—the one that contains the records that you want Route 53 to use when responding to queries for your domain. Route 53 never returns values for records in other hosted zones that have the same name.

Reusable delegation sets

By default, Route 53 assigns a unique set of four name servers (known collectively as a delegation set) to each hosted zone that you create. If you want to create a large number of hosted zones, you can create a reusable delegation set programmatically. (Reusable delegation sets aren't available in the Route 53 console.) Then you can create hosted zones programmatically and assign the same reusable delegation set—the same four name servers—to each hosted zone.

Reusable delegation sets simplify migrating DNS service to Route 53 because you can instruct your domain name registrar to use the same four name servers for all of the domains for which you want to use Route 53 as the DNS service. For more information, see [CreateReusableDelegationSet](#) in the [Amazon Route 53 API Reference](#).

Creating a public hosted zone

A public hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain, such as example.com, and its subdomains (acme.example.com,

zenith.example.com). After you create a hosted zone, you create records that specify how you want to route traffic for the domain and subdomains.

Important

You can create a hosted zone only for a domain that you have permission to administer. Typically, this means that you own the domain, but you might also be developing an application for the domain registrant.

To create a public hosted zone using the Route 53 console

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started** under **DNS management**.
If you're already using Route 53, choose **Hosted zones** in the navigation pane.
3. Choose **Create hosted zone**.
4. In the **Create Hosted Zone** pane, enter the name of the domain that you want to route traffic for. You can also optionally enter a comment.
For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).
5. For **Type**, accept the default value of **Public Hosted Zone**.
6. Choose **Create**.
7. Create records that specify how you want to route traffic for the domain and subdomains. For more information, see [Working with records \(p. 370\)](#).
8. To use records in the new hosted zone to route traffic for your domain, see the applicable topic:
 - If you're making Route 53 the DNS service for a domain that is registered with another domain registrar, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).
 - If the domain is registered with Route 53, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#).

Getting the name servers for a public hosted zone

You get the name servers for a public hosted zone if you want to change the DNS service for your domain registration. For information about how to change your DNS service, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Note

Some registrars only allow you to specify name servers using IP addresses; they don't allow you to specify fully qualified domain names. If your registrar requires using IP addresses, you can get the IP addresses for your name servers using the dig utility (for Mac, Unix, or Linux) or the nslookup utility (for Windows). We rarely change the IP addresses of name servers; if we need to change IP addresses, we'll notify you in advance.

To get the name servers for a hosted zone using the Route 53 console

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, click **Hosted zones**.
3. On the **Hosted zones** page, choose the radio button (not the name) for the hosted zone, then choose **View details**.
4. On the details page for the hosted zone, choose **Hosted zone details**.
5. Make note of the four servers listed for **Name servers**.

Listing public hosted zones

You can use the Amazon Route 53 console to list all of the hosted zones that you created with the current AWS account. For information about how to list hosted zones using the Route 53 API, see [ListHostedZones](#) in the *Amazon Route 53 API Reference*.

To list the public hosted zones associated with an AWS account using the Route 53 console

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**. The page displays a list of the hosted zones that are associated with the AWS account that you are currently signed in with.
3. To filter hosted zones, use the search bar located at the top of the table.

Search behavior depends on whether the hosted zone contains up to 2,000 records or more than 2,000 records:

Up to 2,000 hosted zones

- To display the records that have specific values, click the search bar, choose a property in the dropdown list, and enter a value. You can also enter a value directly in the search bar and press Enter. For example, to display the hosted zones that have a name beginning with **abc**, enter that value in the search bar and press Enter.
- To display only the hosted zones that have the same hosted zone type, select the type in the dropdown list, and enter the type.

More than 2,000 hosted zones

- You can search for properties based on exact domain name, all properties, and type.
- Search using the exact domain name for faster search results.

Viewing DNS query metrics for a public hosted zone

You can view the total number of DNS queries that Route 53 is responding to for a specified public hosted zone or combination of public hosted zones. The metrics appear in CloudWatch, which lets you view a graph, choose the time period that you want to view, and customize the metrics in a variety of other ways. You can also create alarms and configure notifications, so that you're notified when the number of DNS queries in a specified time period go above or below a specified level.

Note

Route 53 automatically sends the number of DNS queries to CloudWatch for all public hosted zones, so you don't need to configure anything before you can view query metrics. There's no charge for DNS query metrics.

Which DNS queries are counted?

Metrics include only the queries that DNS resolvers forward to Route 53. If a DNS resolver has already cached the response to a query (such as the IP address for a load balancer for example.com), the resolver will continue to return the cached response without forwarding the query to Route 53 until the TTL for the corresponding record expires.

Depending on how many DNS queries are submitted for a domain name (example.com) or subdomain name (www.example.com), which resolvers your users are using, and the TTL for the record, DNS query metrics might contain information about only one query out of every several thousand queries that are submitted to DNS resolvers. For more information about how DNS works, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

When do query metrics for a hosted zone start to appear in CloudWatch?

After you create a hosted zone, there's a delay of up to several hours before the hosted zone can appear in CloudWatch. In addition, you must submit a DNS query for a record in the hosted zone so there's data to display.

Metrics are available only in US East (N. Virginia)

To get metrics on the console, you must choose US East (N. Virginia) for the Region. To get metrics using the AWS CLI, you must either leave the AWS Region unspecified, or specify `us-east-1` as the Region. Route 53 metrics aren't available if you choose any other Region.

CloudWatch metric and dimension for DNS queries

For information about the CloudWatch metric and dimension for DNS queries, see [Monitoring hosted zones using Amazon CloudWatch \(p. 628\)](#). For information about CloudWatch metrics, see [Using Amazon CloudWatch metrics](#) in the *Amazon CloudWatch User Guide*.

Getting more detailed data about DNS queries

To get more detailed information about each DNS query that Route 53 responds to, including the following values, you can configure query logging:

- Domain or subdomain that was requested
- Date and time of the request
- DNS record type (such as A or AAAA)
- Route 53 edge location that responded to the DNS query
- DNS response code, such as `NoError` or `ServFail`

For more information, see [Public DNS query logging \(p. 615\)](#).

How to get DNS query metrics

Shortly after you create a hosted zone, Amazon Route 53 starts to send metrics and dimensions once a minute to CloudWatch. You can use the following procedures to view the metrics on the CloudWatch console or view them by using the AWS Command Line Interface (AWS CLI).

Topics

- [Viewing DNS query metrics for a public hosted zone in the CloudWatch console \(p. 343\)](#)
- [Getting DNS query metrics using the AWS CLI \(p. 344\)](#)

Viewing DNS query metrics for a public hosted zone in the CloudWatch console

To view DNS query metrics for public hosted zones in the CloudWatch console, perform the following procedure.

To view DNS query metrics for a public hosted zone on the CloudWatch console

1. Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Metrics**.
3. On the AWS Region list in the upper right corner of the console, choose **US East (N. Virginia)**. Route 53 metrics aren't available if you choose any other AWS Region.
4. On the **All metrics** tab, choose **Route 53**.
5. Choose **Hosted Zone Metrics**.

6. Select the check box for one or more hosted zones that have the metric name **DNSQueries**.
7. On the **Graphed metrics** tab, change the applicable values to view the metrics in the format that you want.

For **Statistic**, choose **Sum** or **SampleCount**; these statistics both display the same value.

Getting DNS query metrics using the AWS CLI

To get DNS query metrics using the AWS CLI, you use the [get-metric-data](#) command. Note the following:

- You specify most values for the command in a separate JSON file. For more information, see [get-metric-data](#).
- The command returns one value for each interval that you specify for **Period** in the JSON file. **Period** is in seconds, so if you specify a five-minute time period and specify 60 for **Period**, you get five values. If you specify a five-minute time period and specify 300 for **Period**, you get one value.
- In the JSON file, you can specify any value for **Id**.
- Either leave the AWS Region unspecified, or specify `us-east-1` as the Region. Route 53 metrics aren't available if you choose any other Region. For more information, see [Configuring the AWS CLI](#) in the [AWS Command Line Interface User Guide](#).

Here's the AWS CLI command that you use to get DNS query metrics for the five-minute time period between 4:01 and 4:07 on May 1, 2019. The `metric-data-queries` parameter references the sample JSON file that follows the command.

```
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
```

Here's the sample JSON file:

```
[  
  {  
    "Id": "my_dns_queries_id",  
    "MetricStat": {  
      "Metric": {  
        "Namespace": "AWS/Route53",  
        "MetricName": "DNSQueries",  
        "Dimensions": [  
          {  
            "Name": "HostedZoneId",  
            "Value": "Z1D633PJN98FT9"  
          }  
        ]  
      },  
      "Period": 60,  
      "Stat": "Sum"  
    },  
    "ReturnData": true  
  }  
]
```

Here's the output from this command. Note the following:

- The start time and end time in the command cover a seven-minute time period, `2019-05-01T04:01:00Z` to `2019-05-01T04:07:00Z`.
- There are only six return values. There's no value for `2019-05-01T04:05:00Z` because there were no DNS queries during that minute.

- The value of `Period` specified in the JSON file is 60 (seconds), so the values are reported in one-minute intervals.

```
{  
    "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"  
            ]  
        }  
    ]  
}
```

Deleting a public hosted zone

This section explains how to delete a public hosted zone using the Amazon Route 53 console.

You can delete a hosted zone only if there are no records other than the default SOA and NS records. If your hosted zone contains other records, you must delete them before you can delete your hosted zone. This prevents you from accidentally deleting a hosted zone that still contains records.

Topics

- [Preventing traffic from being routed to your domain \(p. 345\)](#)
- [Deleting public hosted zones that were created by another service \(p. 346\)](#)
- [Using the Route 53 console to delete a public hosted zone \(p. 346\)](#)

Preventing traffic from being routed to your domain

If you want to keep your domain registration but you want to stop routing internet traffic to your website or web application, we recommend that you delete *records* in the hosted zone instead of deleting the hosted zone.

Important

If you delete a hosted zone, you can't undelete it. You must create a new hosted zone and update the name servers for your domain registration, which can require up to 48 hours to take effect. In addition, if you delete a hosted zone, someone could hijack the domain and route traffic to their own resources using your domain name.

If you delegated responsibility for a subdomain to a hosted zone and you want to delete the child hosted zone, you must also update the parent hosted zone by deleting the NS record that has the same name as the child hosted zone. For example, if you want to delete the hosted zone acme.example.com, you must also delete the NS record acme.example.com in the example.com hosted zone. We recommend that you delete the NS record first, and wait for the duration of the

TTL on the NS record before you delete the child hosted zone. This ensures that someone can't hijack the child hosted zone during the period that DNS resolvers still have the name servers for the child hosted zone cached.

If you want to avoid the monthly charge for the hosted zone, you can transfer DNS service for the domain to a free DNS service. When you transfer DNS service, you have to update the name servers for the domain registration. If the domain is registered with Route 53, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#) for information about how to replace Route 53 name servers with name servers for the new DNS service. If the domain is registered with another registrar, use the method provided by the registrar to update name servers for the domain registration. For more information, perform an internet search on "free DNS service."

Deleting public hosted zones that were created by another service

If a hosted zone was created by another service, you can't delete it using the Route 53 console. Instead, you need to use the applicable process for the other service:

- **AWS Cloud Map** – To delete a hosted zone that AWS Cloud Map created when you created a public DNS namespace, delete the namespace. AWS Cloud Map deletes the hosted zone automatically. For more information, see [Deleting namespaces](#) in the *AWS Cloud Map Developer Guide*.
- **Amazon Elastic Container Service (Amazon ECS) Service Discovery** – To delete a public hosted zone that Amazon ECS created when you created a service using service discovery, delete the Amazon ECS services that are using the namespace, and delete the namespace. For more information, see [Deleting a service](#) in the *Amazon Elastic Container Service Developer Guide*.

Using the Route 53 console to delete a public hosted zone

To use the Route 53 console to delete a public hosted zone, perform the following procedure.

To delete a public hosted zone using the Route 53 console

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Confirm that the hosted zone that you want to delete contains only an NS and an SOA record. If it contains additional records, delete them. You will also need to disable DNSSEC signing:
 - a. Choose the name of the hosted zone that you want to delete.
 - b. On the Record page, if the list of records includes any records for which the value of the **Type** column is something other than NS or SOA, choose the row, and choose **Delete**.

To select multiple, consecutive records, choose the first row, press and hold the **Shift** key, and choose the last row. To select multiple, non-consecutive records, choose the first row, press and hold the **Ctrl** key, and choose the remaining rows.

Note

If you created any NS records for subdomains in the hosted zone, delete those records, too.

3. On the **Hosted zones** page, choose the row for the hosted zone that you want to delete.
4. Choose **Delete**.
5. Type the confirmation key and choose **Delete**.
6. If you want to make the domain unavailable on the internet, we recommend that you transfer DNS service to a free DNS service and then delete the Route 53 hosted zone. This prevents future DNS queries from possibly being misrouted.

If the domain is registered with Route 53, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#) for information about how to replace Route 53 name servers with name servers for

the new DNS service. If the domain is registered with another registrar, use the method provided by the registrar to change name servers for the domain.

Note

If you're deleting a hosted zone for a subdomain (acme.example.com), you don't need to change name servers for the domain (example.com).

Checking DNS responses from Route 53

If you created an Amazon Route 53 hosted zone for your domain, you can use the DNS checking tool in the console to see how Route 53 will respond to DNS queries if you configure your domain to use Route 53 as your DNS service. For geolocation, geoproximity, and latency records, you can also simulate queries from a particular DNS resolver and/or client IP address to find out what response Route 53 would return.

Important

The tool doesn't submit queries to the Domain Name System, it only responds based on the settings in the records in the hosted zone. The tool returns the same information regardless of whether the hosted zone is currently being used to route traffic for the domain.

The DNS checking tool works only for public hosted zones.

Topics

- [Using the checking tool to see how Amazon Route 53 responds to DNS queries \(p. 347\)](#)
- [Using the checking tool to simulate queries from specific IP addresses \(geolocation and latency records only\) \(p. 348\)](#)

Using the checking tool to see how Amazon Route 53 responds to DNS queries

You can use the tool to see what response Amazon Route 53 returns in response to a DNS query for a record.

To use the checking tool to see how Route 53 responds to DNS queries

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted Zones**.
3. On the **Hosted Zones** page, choose the name of a hosted zone. The console displays the list of records for that hosted zone.
4. To go directly to the **Check response from Route 53** page, choose **Test record**.
5. Specify the following values:
 - The name of the record, excluding the name of the hosted zone. For example, to check **www.example.com**, enter **www**. To check **example.com**, leave the **Record name** field blank.
 - The type of the record that you want to check, such as **A** or **CNAME**.
6. Choose **Get Response**.
7. The **Response returned by Route 53** section includes the following values:

DNS response code

A code that indicates whether the query was valid or not. The most common response code is **NOERROR**, meaning that the query was valid. If the response is not valid, Route 53 returns a response code that explains why not. For a list of possible response codes, see [DNS RCODES](#) on the IANA website.

Protocol

The protocol that Amazon Route 53 used to respond to the query, either **UDP** or **TCP**.

Response returned by Route 53

The value that Route 53 would return to a web application. The value is one of the following:

- For non-alias records, the response contains the value or values in the record.
- For multiple records that have the same name and type, which includes weighted, latency, geolocation, and failover, the response contains the value from the appropriate record, based on the request.
- For alias records that refer to AWS resources other than another record, the response contains an IP address or a domain name for the AWS resource, depending on the type of resource.
- For alias records that refer to other records, the response contains the value or values from the referenced record.

Using the checking tool to simulate queries from specific IP addresses (geolocation and latency records only)

If you have created latency or geolocation records, you can use the checking tool to simulate queries from the IP address for a DNS resolver and a client.

To use the checking tool to simulate queries from specified IP addresses

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted Zones**.
3. On the **Hosted Zones** page, choose the name of a hosted zone. The console displays the list of records for that hosted zone.
4. To go directly to the **Check response from Route 53** page, choose **Test record set**.

To go to the **Check response from Route 53** page for a specific record, choose the check box for that record and choose **Test record set**.

5. If you chose **Test record set** without first choosing a record, specify the following values:
 - The name of the record, excluding the name of the hosted zone. For example, to check **www.example.com**, enter **www**. To check **example.com**, leave the **Record name** field blank.
 - The type of the record that you want to check, such as **A** or **CNAME**.
6. Specify the applicable values:

Resolver IP address

Specify an IPv4 or IPv6 address to simulate the location of the DNS resolver that a client uses to make requests. This is useful for testing latency and geolocation records. If you omit this value, the tool uses the IP address of a DNS resolver in the AWS US East (N. Virginia) Region (us-east-1).

EDNS0 client subnet IP

If the resolver supports EDNS0, enter the client subnet IP for an IP address in the applicable geographic location, for example, **192.0.2.0** or **2001:db8:85a3::8a2e:370:7334**.

Subnet mask

If you specify an IP address for **EDNS0 client subnet IP**, you can optionally specify the number of bits of the IP address that you want the checking tool to include in the DNS query. For example, if you specify **192.0.2.44** for **EDNS0 client subnet IP** and **24** for **Subnet mask**, the

checking tool will simulate a query from **192.0.2.0/24**. The default value is 24 bits for IPv4 addresses and 64 bits for IPv6 addresses.

7. Choose **Get Response**.
8. The **Response returned by Route 53** section includes the following values:

DNS query sent to Route 53

The query, in [BIND format](#), that the checking tool sent to Route 53. This is the same format that a web application would use to send a query. The three values are typically the name of the record, **IN** (for internet), and the type of the record.

DNS response code

A code that indicates whether the query was valid or not. The most common response code is **NOERROR**, meaning that the query was valid. If the response is not valid, Route 53 returns a response code that explains why not. For a list of possible response codes, see [DNS RCODES](#) on the IANA website.

Protocol

The protocol that Amazon Route 53 used to respond to the query, either **UDP** or **TCP**.

Response returned by Route 53

The value that Route 53 would return to a web application. The value is one of the following:

- For non-alias records, the response contains the value or values in the record.
- For multiple records that have the same name and type, which includes weighted, latency, geolocation, and failover, the response contains the value from the appropriate record, based on the request.
- For alias records that refer to AWS resources other than another record, the response contains an IP address or a domain name for the AWS resource, depending on the type of resource.
- For alias records that refer to other records, the response contains the value or values from the referenced record.

Configuring white-label name servers

Each Amazon Route 53 hosted zone is associated with four name servers, known collectively as a delegation set. By default, the name servers have names like ns-2048.awsdns-64.com. If you want the domain name of your name servers to be the same as the domain name of your hosted zone, for example, ns1.example.com, you can configure white-label name servers, also known as vanity name servers or private name servers.

The following steps explain how to configure one set of four white-label name servers that you can reuse for multiple domains. For example, suppose you own the domains example.com, example.org, and example.net. With these steps, you can configure white-label name servers for example.com and reuse them for example.org and example.net.

Topics

- [Step 1: Create a Route 53 reusable delegation set \(p. 350\)](#)
- [Step 2: Create or recreate Amazon Route 53 hosted zones, and change the TTL for NS and SOA records \(p. 350\)](#)
- [Step 3: Recreate records for your hosted zones \(p. 350\)](#)
- [Step 4: Get IP addresses \(p. 351\)](#)
- [Step 5: Create records for white-label name servers \(p. 352\)](#)
- [Step 6: Update NS and SOA records \(p. 353\)](#)
- [Step 7: Create glue records and change the registrar's name servers \(p. 353\)](#)

- Step 8: Monitor traffic for the website or application (p. 354)
- Step 9: Change TTLs back to their original values (p. 354)
- Step 10: (Optional) contact recursive DNS services (p. 354)

Step 1: Create a Route 53 reusable delegation set

White-label name servers are associated with a Route 53 reusable delegation set. You can use white-label name servers for a hosted zone only if the hosted zone and the reusable delegation set were created by the same AWS account.

To create a reusable delegation set, you can use the Route 53 API, the AWS CLI, or one of the AWS SDKs. For more information, see the following documentation:

- **Route 53 API** – See [CreateReusableDelegationSet](#) in the *Amazon Route 53 API Reference*
- **AWS CLI** – See [create-reusable-delegation-set](#) in the *AWS CLI Command Reference*
- **AWS SDKs** See the applicable SDK documentation on the [AWS Documentation](#) page

Step 2: Create or recreate Amazon Route 53 hosted zones, and change the TTL for NS and SOA records

Create or recreate Amazon Route 53 hosted zones:

- **If you aren't currently using Route 53 as the DNS service for the domains for which you want to use white-label name servers** – Create the hosted zones and specify the reusable delegation set that you created in the previous step with each hosted zone. For more information, see [CreateHostedZone](#) in the *Amazon Route 53 API Reference*.
- **If you are using Route 53 as the DNS service for the domains for which you want to use white-label name servers** – You must recreate the hosted zones for which you want to use white-label name servers, and specify the reusable delegation set that you created in the previous step for each hosted zone.

Important

You cannot change the name servers that are associated with an existing hosted zone. You can associate a reusable delegation set with a hosted zone only when you create the hosted zone.

When you create the hosted zones and before you try to access the resources for the corresponding domains, change the following TTL values for each hosted zone:

- Change the TTL for the NS record for the hosted zone to 60 seconds or less.
- Change the minimum TTL for the SOA record for the hosted zone to 60 seconds or less. This is the last value in the SOA record.

If you accidentally give your registrar the wrong IP addresses for your white-label name servers, your website will become unavailable and remain unavailable for the duration of the TTL after you correct the problem. By setting a low TTL, you reduce the amount of time that your website is unavailable.

For more information about creating hosted zones and specifying a reusable delegation set for the name servers for the hosted zones, see [CreateHostedZone](#) in the *Amazon Route 53 API Reference*.

Step 3: Recreate records for your hosted zones

Create records in the hosted zones that you created in Step 2:

- **If you're migrating DNS service for your domains to Amazon Route 53** – You might be able to create records by importing information about your existing records. For more information, see [Creating records by importing a zone file \(p. 438\)](#).
- **If you're replacing existing hosted zones so that you can use white-label name servers** – In the new hosted zones, recreate the records that appear in your current hosted zones. Route 53 doesn't provide a method of exporting records from a hosted zone, but some third-party vendors do. You can then use the Route 53 import feature to import non-alias records for which the routing policy is simple. There is no way to export and re-import alias records or records for which the routing policy is anything other than simple.

For information about creating records by using the Route 53 API, see [CreateHostedZone](#) in the *Amazon Route 53 API Reference*. For information about creating records by using the Route 53 console, see [Working with records \(p. 370\)](#).

Step 4: Get IP addresses

Get the IPv4 and IPv6 addresses of the name servers in the reusable delegation set, and fill in the following table.

Name of a name server in your reusable delegation set (example: Ns-2048.awsdns-64.com)	IPv4 and IPv6 addresses	Name that you want to assign to the white-label name server (example: ns1.example.com)
	IPv4: IPv6:	

For example, suppose the four name servers for your reusable delegation set are:

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Here are the Linux and Windows commands that you'd run to get the IP addresses for the first of your four name servers:

dig commands for 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
```

nslookup command for 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
```

Step 5: Create records for white-label name servers

In the hosted zone that has the same name (such as example.com) as the domain name of the white-label name servers (such as ns1.example.com), create eight records:

- One A record for each white-label name server
- One AAAA record for each white-label name server

Important

If you're using the same white-label name servers for two or more hosted zones, do not perform this step for the other hosted zones.

For each record, specify the following values. Refer to the table that you filled in for the previous step:

Routing policy

Specify Simple routing.

Record name

The name that you want to assign to one of your white-label name servers, for example, ns1.example.com. For the prefix (ns1 in this example), you can use any value that is valid in a domain name.

Value/Route traffic to

The IPv4 or IPv6 address of one of the Route 53 name servers in your reusable delegation set.

Important

If you specify the wrong IP addresses when you created records for your white-label name servers, your website or web application will become unavailable on the internet when you perform subsequent steps. Even if you correct the IP addresses immediately, your website or web application will remain unavailable for the duration of the TTL.

Record type

Specify A when you're creating records for the IPv4 addresses.

Specify AAAA when you're creating records for the IPv6 addresses.

TTL (seconds)

This value is the amount of time that DNS resolvers cache the information in this record before forwarding another DNS query to Route 53. We recommend that you specify an initial value of 60 seconds or less, so that you can recover quickly if you accidentally specify incorrect values in these records.

Step 6: Update NS and SOA records

Update SOA and NS records in the hosted zones that you want to use white-label name servers for. Perform Step 6 through Step 8 for one hosted zone and the corresponding domain at a time, then repeat for another hosted zone and domain.

Important

Start with the Amazon Route 53 hosted zone that has the same domain name (such as example.com) as the white-label name servers (such as ns1.example.com).

1. Update the SOA record by replacing the name of the Route 53 name server with the name of one of your white-label name servers

Example

Replace the name of the Route 53 name server:

`ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60`

with the name of one of your white-label name servers:

`ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60`

Note

You changed the last value, the time to live (TTL), in [Step 2: Create or recreate Amazon Route 53 hosted zones, and change the TTL for NS and SOA records \(p. 350\)](#).

For information about updating records by using the Route 53 console, see [Editing records \(p. 440\)](#).

2. In the NS record, make note of the names of the current name servers for the domain, so you can revert to these name servers if necessary.
3. Update the NS record. Replace the name of the Route 53 name servers with the names of your four white-label name servers, for example, ns1.example.com, ns2.example.com, ns3.example.com, and ns4.example.com.

Step 7: Create glue records and change the registrar's name servers

Use the method provided by the registrar to create glue records and change the registrar's name servers:

1. Add glue records:

- **If you're updating the domain that has the same domain name as the white-label name servers**
– Create four glue records for which the names and IP addresses match the values that you got in step 4. Include both the IPv4 and the IPv6 address for a white-label name server in the corresponding glue record, for example:

`ns1.example.com - IP addresses = 192.0.2.117 and 2001:db8:85a3::8a2e:370:7334`

Registrars use a variety of terminology for glue records. You might also see this referred to as registering new name servers or something similar.

- **If you're updating another domain** – If Route 53 is your DNS service, you must first complete the step in the previous bullet and create the glue records that match the domain name. Then skip to step 2 in this procedure.

2. Change the name servers for the domain to the names of your white-label name servers.

If you're using Amazon Route 53 as your DNS service, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#).

Step 8: Monitor traffic for the website or application

Monitor the traffic for the website or application for which you created glue records and changed name servers in Step 7:

- **If the traffic stops** – Use the method provided by the registrar to change the name servers for the domain back to the previous Route 53 name servers. These are the name servers that you made note of in step 6b. Then determine what went wrong.
- **If the traffic is unaffected** – Repeat Step 6 through Step 8 for the rest of the hosted zones for which you want to use the same white-label name servers.

Step 9: Change TTLs back to their original values

For all of the hosted zones that are now using white-label name servers, change the following values:

- Change the TTL for the NS record for the hosted zone to a more typical value for NS records, for example, 172800 seconds (two days).
- Change the minimum TTL for the SOA record for the hosted zone to a more typical value for SOA records, for example, 900 seconds. This is the last value in the SOA record.

Step 10: (Optional) contact recursive DNS services

Optional If you're using Amazon Route 53 geolocation routing, contact the recursive DNS services that support the edns-client-subnet extension of EDNS0, and give them the names of your white-label name servers. This ensures that these DNS services will continue to route DNS queries to the optimal Route 53 location based on the approximate geographical location that the query came from.

NS and SOA records that Amazon Route 53 creates for a public hosted zone

For each public hosted zone that you create, Amazon Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record. You rarely need to change these records.

Topics

- [The name server \(NS\) record \(p. 354\)](#)
- [The start of authority \(SOA\) record \(p. 355\)](#)

The name server (NS) record

Amazon Route 53 automatically creates a name server (NS) record that has the same name as your hosted zone. It lists the four name servers that are the authoritative name servers for your hosted zone. Except in rare circumstances, we recommend that you don't add, change, or delete name servers in this record.

The following examples show the format for the names of Route 53 name servers (these are examples only; don't use them when you're updating your registrar's name server records):

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

To get the list of name servers for your hosted zone:

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, click **Hosted zones**.
3. On the **Hosted zones** page, choose the radio button (not the name) for the hosted zone, then choose **View details**.
4. On the details page for the hosted zone, choose **Hosted zone details**.
5. Make note of the four servers listed for **Name servers**.

For information about migrating DNS service from another DNS service provider to Route 53, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

The start of authority (SOA) record

The start of authority (SOA) record identifies the base DNS information about the domain, for example:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

A SOA record includes the following elements:

- The Route 53 name server that created the SOA record, for example, ns-2048.awsdns-64.net.
- The email address of the administrator. The @ symbol is replaced by a period, for example, hostmaster.example.com. The default value is an amazon.com email address that is not monitored.
- A serial number that you can optionally increment whenever you update a record in the hosted zone. Route 53 doesn't increment the number automatically. (The serial number is used by DNS services that support secondary DNS.) In the example, this value is 1.
- A refresh time in seconds that secondary DNS servers wait before querying the primary DNS server's SOA record to check for changes. In the example, this value is 7200.
- The retry interval in seconds that a secondary server waits before retrying a failed zone transfer. Normally, the retry time is less than the refresh time. In the example, this value is 900 (15 minutes).
- The time in seconds that a secondary server will keep trying to complete a zone transfer. If this time elapses before a successful zone transfer, the secondary server will stop answering queries because it considers its data too old to be reliable. In the example, this value is 1209600 (two weeks).
- The minimum time to live (TTL). This value helps define the length of time that recursive resolvers should cache the following responses from Route 53:

NXDOMAIN

There is no record of any type with the name that is specified in the DNS query, such as example.com. There also are no records that are children of the name that is specified in the DNS query, such as zenith.example.com.

NODATA

There is at least one record with the name that is specified in the DNS query, but none of those records have the type (such as A) that is specified in the DNS query.

When a DNS resolver caches an NXDOMAIN or NODATA response, this is referred to as *negative caching*.

The duration of negative caching is the lesser of the following values:

- This value—the minimum TTL in the SOA record. In the example, the value is 86400 (one day).
- The value of the TTL for the SOA record. The default value is 900 seconds. For information about changing this value, see [Editing records \(p. 440\)](#).

When Route 53 responds to DNS queries with an NXDOMAIN or NODATA response (a negative response), you're charged the rate for standard queries. (See "Queries" in [Amazon Route 53 Pricing](#). If

you're concerned about the cost of negative responses, one option is to change the TTL for the SOA record, the minimum TTL in the SOA record (this value), or both. Note that increasing these TTLs, which apply to negative responses for the entire hosted zone, can have both positive and negative effects:

- DNS resolvers on the internet cache the non-existence of records for longer periods, which reduces the number of queries that are forwarded to Route 53. This reduces the Route 53 charge for DNS queries.
- However, if you ever erroneously delete a valid record and later recreate it, DNS resolvers will cache the negative response (this record doesn't exist) for a longer period. This lengthens the amount of time that your customers or users can't reach the corresponding resource, such as a web server for acme.example.com.

To find your SOA records in Route 53

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Select the linked name of the domain for which you want to view records.
4. On the **Records** section you can see all the records listed and you can also filter records to find your SOA value.

Working with private hosted zones

A *private hosted zone* is a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs that you create with the Amazon VPC service. Here's how private hosted zones work:

1. You create a private hosted zone, such as example.com, and specify the VPCs that you want to associate with the hosted zone.
2. You create records in the hosted zone that determine how Route 53 responds to DNS queries for your domain and subdomains within and among your VPCs. For example, suppose you have a database server that runs on an EC2 instance in one of the VPCs that you associated with your private hosted zone. You create an A or AAAA record, such as db.example.com, and you specify the IP address of the database server.

For more information about records, see [Working with records \(p. 370\)](#). For information about the Amazon VPC requirements for using private hosted zones, see [Using private hosted zones in the Amazon VPC User Guide](#).

3. When an application submits a DNS query for db.example.com, Route 53 returns the corresponding IP address. The application must also be running on an EC2 instance in one of the VPCs that you associated with the example.com private hosted zone.
4. The application uses the IP address that it got from Route 53 to establish a connection with the database server.

If you want to route traffic for your domain on the internet, you use a Route 53 *public* hosted zone. For more information, see [Working with public hosted zones \(p. 339\)](#).

Topics

- [Considerations when working with a private hosted zone \(p. 357\)](#)
- [Creating a private hosted zone \(p. 359\)](#)
- [Listing private hosted zones \(p. 360\)](#)
- [Associating more VPCs with a private hosted zone \(p. 361\)](#)

- [Associating an Amazon VPC and a private hosted zone that you created with different AWS accounts \(p. 361\)](#)
- [Disassociating VPCs from a private hosted zone \(p. 362\)](#)
- [Deleting a private hosted zone \(p. 362\)](#)

Considerations when working with a private hosted zone

When using private hosted zones, note the following considerations.

- [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 Resolver rules](#)
- [Delegating responsibility for a subdomain](#)
- [Custom DNS servers](#)
- [Required IAM permissions](#)

Amazon VPC settings

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

For more information, see [Updating DNS support for your VPC](#) in the *Amazon VPC User Guide*.

Route 53 health checks

In a private hosted zone, you can associate Route 53 health checks only with failover, multivalue answer, weighted, latency and, geolocation records. For information about associating health checks with failover records, see [Configuring failover in a private hosted zone \(p. 550\)](#).

Supported routing policies for records in a private hosted zone

You can use the following routing policies when you create records in a private hosted zone:

- [Simple routing \(p. 371\)](#)
- [Failover routing \(p. 372\)](#)
- [Multivalue answer routing \(p. 378\)](#)
- [Weighted routing \(p. 378\)](#)
- [Latency-based routing \(p. 377\)](#)
- [Geolocation routing \(p. 372\)](#)

Creating records in a private hosted zone using other routing policies is not supported.

Split-view DNS

You can use Route 53 to configure split-view DNS, also known as split-horizon DNS. In split-view DNS, you use the same domain name (example.com) for internal uses (accounting.example.com) and external uses, such as your public website (www.example.com). You might also want to use the same subdomain name internally and externally, but serve different content or require different authentication for internal and external users.

To configure split-view DNS, you perform the following steps:

1. Create public and private hosted zones that have the same name. (Split-view DNS still works if you're using another DNS service for the public hosted zone.)
2. Associate one or more Amazon VPCs with the private hosted zone. Route 53 Resolver uses the private hosted zone to route DNS queries in the specified VPCs.
3. Create records in each hosted zone. Records in the public hosted zone control how internet traffic is routed, and records in the private hosted zone control how traffic is routed in your Amazon VPCs.

If you need to perform name resolution of both your VPC and on-premises workloads, you can use Route 53 Resolver. For more information, see [Resolving DNS queries between VPCs and your network \(p. 471\)](#).

Public and private hosted zones that have overlapping namespaces

If you have private and public hosted zones that have overlapping namespaces, such as example.com and accounting.example.com, Resolver routes traffic based on the most specific match. When users are logged into an EC2 instance in an Amazon VPC that you have associated with the private hosted zone, here's how Route 53 Resolver handles DNS queries:

1. Resolver evaluates whether the name of the private hosted zone matches the domain name in the request, such as accounting.example.com. A match is defined as either of the following:
 - An identical match
 - The name of the private hosted zone is a parent of the domain name in the request. For example, suppose the domain name in the request is the following:

seattle.accounting.example.com

The following hosted zones match because they're parents of seattle.accounting.example.com:

- **accounting.example.com**
- **example.com**

If there's no matching private hosted zone, then Resolver forwards the request to a public DNS resolver, and your request is resolved as a regular DNS query.

2. If there's a private hosted zone name that matches the domain name in the request, the hosted zone is searched for a record that matches the domain name and DNS type in the request, such as an A record for accounting.example.com.

Note

If there's a matching private hosted zone but there's no record that matches the domain name and type in the request, Resolver doesn't forward the request to a public DNS resolver. Instead, it returns NXDOMAIN (non-existent domain) to the client.

Private hosted zones that have overlapping namespaces

If you have two or more private hosted zones that have overlapping namespaces, such as example.com and accounting.example.com, Resolver routes traffic based on the most specific match.

Note

If you have a private hosted zone (example.com) and a Route 53 Resolver rule that routes traffic to your network for the same domain name, the Resolver rule takes precedence. See [Private hosted zones and Route 53 Resolver rules](#).

When users are logged into an EC2 instance in an Amazon VPC that you have associated with all of the private hosted zones, here's how Resolver handles DNS queries:

1. Resolver evaluates whether the domain name in the request, such as accounting.example.com, matches the name of one of the private hosted zones.
2. If there is no hosted zone that exactly matches the domain name in the request, Resolver checks for a hosted zone that has a name that is the parent of the domain name in the request. For example, suppose the domain name in the request is the following:

`seattle.accounting.example.com`

The following hosted zones match because they're parents of `seattle.accounting.example.com`:

- `accounting.example.com`
- `example.com`

Resolver chooses `accounting.example.com` because it's more specific than `example.com`.

3. Resolver searches the `accounting.example.com` hosted zone for a record that matches the domain name and DNS type in the request, such as an A record for `seattle.accounting.example.com`.

If there's no record that matches the domain name and type in the request, Resolver returns NXDOMAIN (non-existent domain) to the client.

Private hosted zones and Route 53 Resolver rules

If you have a private hosted zone (`example.com`) and a Resolver rule that routes traffic to your network for the same domain name, the Resolver rule takes precedence.

For example, suppose you have the following configuration:

- You have a private hosted zone called `example.com`, and you associate it with a VPC.
- You create a Route 53 Resolver rule that forwards traffic for `example.com` to your network, and you associate the rule with the same VPC.

In this configuration, the Resolver rule takes precedence over the private hosted zone. DNS queries are forwarded to your network instead of being resolved based on the records in the private hosted zone.

Delegating responsibility for a subdomain

You cannot create NS records in a private hosted zone to delegate responsibility for a subdomain.

Custom DNS servers

If you have configured custom DNS servers on Amazon EC2 instances in your VPC, you must configure those DNS servers to route your private DNS queries to the IP address of the Amazon-provided DNS servers for your VPC. This IP address is the IP address at the base of the VPC network range "plus two." For example, if the CIDR range for your VPC is 10.0.0.0/16, the IP address of the DNS server is 10.0.0.2.

If you want to route DNS queries between VPCs and your network, you can use Resolver. For more information, see [Resolving DNS queries between VPCs and your network \(p. 471\)](#).

Required IAM permissions

To create private hosted zones, you need to grant IAM permissions for Amazon EC2 actions in addition to permissions for Route 53 actions. For more information, see [Required permissions for actions on private hosted zones \(p. 597\)](#).

Creating a private hosted zone

A private hosted zone is a container for records for a domain that you host in one or more Amazon virtual private clouds (VPCs). You create a hosted zone for a domain (such as `example.com`), and then you create records to tell Amazon Route 53 how you want traffic to be routed for that domain within and among your VPCs.

Important

When you create a private hosted zone, you must associate a VPC with the hosted zone, and the VPC that you specify must have been created by using the same account that you're using

to create the hosted zone. After you create the hosted zone, you can associate additional VPCs with it, including VPCs that you created by using a different AWS account.

To associate VPCs that you created by using one account with a private hosted zone that you created by using a different account, you must authorize the association and then make the association programmatically. For more information, see [Associating an Amazon VPC and a private hosted zone that you created with different AWS accounts \(p. 361\)](#).

For information about creating a private hosted zone by using the Route 53 API, see the [Amazon Route 53 API Reference](#).

To create a private hosted zone using the Route 53 console

1. For each VPC that you want to associate with the Route 53 hosted zone, change the following VPC settings to true:

- `enableDnsHostnames`
- `enableDnsSupport`

For more information, see [Updating DNS support for your VPC](#) in the *Amazon VPC User Guide*.

2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. If you're new to Route 53, choose **Get started**

If you're already using Route 53, choose **Hosted zones** in the navigation pane.

4. Choose **Create hosted zone**.
5. In the **Create private hosted zone** pane, enter a domain name and, optionally, a comment.

For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).

6. In the **Type** list, choose **Private hosted zone**.
7. In the **VPC ID** list, choose the VPC that you want to associate with the hosted zone.

Note

If the console displays the following message, you're trying to associate a hosted zone that uses the same name space as that of another hosted zone within the same VPC:
"A conflicting domain is already associated with the given VPC or Delegation Set."
For example, if hosted zone A and hosted zone B both use the name space `example.com`, you can't associate both hosted zones with the same VPC.

8. Choose **Create hosted zone**.

Listing private hosted zones

You can use the Amazon Route 53 console to list all of the hosted zones that you created with the current AWS account. For information about how to list hosted zones using the Route 53 API, see [ListHostedZones](#) in the *Amazon Route 53 API Reference*.

To list the hosted zones associated with an AWS account

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.

The **Hosted Zones** page automatically displays a list of all of the hosted zones that were created using the current AWS account. The **Type** column indicates whether a hosted zone is private or public. Choose the column heading to group all private hosted zones and all public hosted zones.

Associating more VPCs with a private hosted zone

You can use the Amazon Route 53 console to associate more VPCs with a private hosted zone if you created the hosted zone and the VPCs by using the same AWS account.

Important

If you want to associate VPCs that you created by using one account with a private hosted zone that you created by using a different account, you first must authorize the association. In addition, you can't use the AWS console either to authorize the association or associate the VPCs with the hosted zone. For more information, see [Associating an Amazon VPC and a private hosted zone that you created with different AWS accounts \(p. 361\)](#).

For information about how to associate more VPCs with a private hosted zone using the Route 53 API, see [AssociateVPCWithHostedZone](#) in the *Amazon Route 53 API Reference*.

To associate additional VPCs with a private hosted zone using the Route 53 console

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Choose the radio button for the private hosted zone that you want to associate more VPCs with.
4. Choose **Edit**.
5. Choose **Add VPC**.
6. Choose the Region and the ID of the VPC that you want to associate with this hosted zone.
7. To associate more VPCs with this hosted zone, repeat steps 5 and 6.
8. Choose **Save changes**.

Associating an Amazon VPC and a private hosted zone that you created with different AWS accounts

If you want to associate a VPC that you created with one AWS account with a private hosted zone that you created with a different account, perform the following procedure:

To associate an Amazon VPC and a private hosted zone that you created with different AWS accounts

1. Using the account that created the hosted zone, authorize the association of the VPC with the private hosted zone by using one of the following methods:
 - **AWS CLI** – See [create-vpc-association-authorization](#) in the *AWS CLI Command Reference*
 - **AWSSDK or AWS Tools for Windows PowerShell** – See the applicable documentation on the [AWS Documentation](#) page
 - **Amazon Route 53 API** – See [CreateVPCAssociationAuthorization](#) in the *Amazon Route 53 API Reference*

Note the following:

- If you want to associate multiple VPCs that you created with one account with a hosted zone that you created with a different account, you must submit one authorization request for each VPC.
- When you authorize the association, you must specify the hosted zone ID, so the private hosted zone must already exist.
- You can't use the Route 53 console either to authorize the association of a VPC with a private hosted zone or to make the association.

2. Using the account that created the VPC, associate the VPC with the hosted zone. As with authorizing the association, you can use the AWS SDK, Tools for Windows PowerShell, the AWS CLI, or the Route 53 API. If you're using the API, use the [AssociateVPCWithHostedZone](#) action.
3. *Recommended* – Delete the authorization to associate the VPC with the hosted zone. Deleting the authorization does not affect the association, it just prevents you from reassociating the VPC with the hosted zone in the future. If you want to reassociate the VPC with the hosted zone, you'll need to repeat steps 1 and 2 of this procedure.

If you don't delete the authorization, the other account can re-associate the VPC at any time because the authorization is still in place. For more information, see [delete-vpc-association-authorization](#).

Note

For the maximum number of authorizations that you can create, see [Quotas on entities \(p. 671\)](#).

Disassociating VPCs from a private hosted zone

You can use the Amazon Route 53 console to disassociate VPCs from a private hosted zone. This causes Route 53 to stop routing traffic using records in the hosted zone for DNS queries that originate in the VPC. For example, if the example.com hosted zone is associated with a VPC and you disassociate the hosted zone from that VPC, Route 53 stops resolving DNS queries for example.com or any of the other records in the example.com hosted zone.

Note

You can't disassociate the last VPC from a private hosted zone. If you want to disassociate that VPC, you must first associate another VPC with the hosted zone.

To disassociate VPCs from a private hosted zone

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Choose the radio button for the private hosted zone that you want to disassociate one or more VPCs from.
4. Choose **Edit**.
5. Choose **Remove VPC** next to the VPC that you want to disassociate from this hosted zone.
6. Choose **Save changes**.

Deleting a private hosted zone

This section explains how to delete a private hosted zone using the Amazon Route 53 console.

You can delete a private hosted zone only if there are no records other than the default SOA and NS records. If your hosted zone contains other records, you must delete them before you can delete your hosted zone. This prevents you from accidentally deleting a hosted zone that still contains records.

Topics

- [Deleting private hosted zones that were created by another service \(p. 362\)](#)
- [Using the Route 53 console to delete a private hosted zone \(p. 363\)](#)

Deleting private hosted zones that were created by another service

If a private hosted zone was created by another service, you can't delete it using the Route 53 console. Instead, you need to use the applicable process for the other service:

- **AWS Cloud Map** – To delete a hosted zone that AWS Cloud Map created when you created a private DNS namespace, delete the namespace. AWS Cloud Map deletes the hosted zone automatically. For more information, see [Deleting namespaces](#) in the *AWS Cloud Map Developer Guide*.
- **Amazon Elastic Container Service (Amazon ECS) Service Discovery** – To delete a private hosted zone that Amazon ECS created when you created a service using service discovery, delete the Amazon ECS services that are using the namespace, and delete the namespace. For more information, see [Deleting a service](#) in the *Amazon Elastic Container Service Developer Guide*.

Using the Route 53 console to delete a private hosted zone

To use the Route 53 console to delete a private hosted zone, perform the following procedure.

To delete a private hosted zone using the Route 53 console

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Confirm that the hosted zone that you want to delete contains only an NS and an SOA record. If it contains additional records, delete them:
 - a. Choose the name of the hosted zone that you want to delete.
 - b. On the **Record** page, if the list of records includes any records for which the value of the **Type** column is something other than **NS** or **SOA**, choose the row, and choose **Delete**.

To select multiple, consecutive records, choose the first row, press and hold the **Shift** key, and choose the last row. To select multiple, non-consecutive records, choose the first row, press and hold the **Ctrl** key, and choose the remaining rows.
3. On the Hosted Zones page, choose the row for the hosted zone that you want to delete.
4. Choose **Delete**.
5. Type the confirmation key and choose **Delete**.

Migrating a hosted zone to a different AWS account

If you want to migrate a hosted zone from one AWS account to a different account, you can programmatically list the records in the old hosted zone, edit the output, and then programmatically create records in a new hosted zone using the edited output. Note the following:

- If you have only a few records, you can also use the Route 53 console to create records in the new hosted zone. For more information, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).
- Some procedures use the AWS Command Line Interface (AWS CLI). You can also perform those procedures by using one of the AWS SDKs, the Amazon Route 53 API, or AWS Tools for Windows PowerShell. For this topic, we use the AWS CLI because it's easier for small numbers of hosted zones.
- You can also use this process to create records in a new hosted zone that has a different name than an existing hosted zone but that has the same records.
- You can't migrate alias records that route traffic to traffic policy instances.

Topics

- [Step 1: Install or upgrade the AWS CLI \(p. 364\)](#)
- [Step 2: Create the new hosted zone \(p. 364\)](#)
- [Step 3: Create a file that contains the records that you want to migrate \(p. 364\)](#)
- [Step 4: Edit the records that you want to migrate \(p. 365\)](#)
- [Step 5: Split large files into smaller files \(p. 367\)](#)

- Step 6: Create records in the new hosted zone (p. 367)
- Step 7: Compare records in the old and new hosted zones (p. 368)
- Step 8: Update the domain registration to use name servers for the new hosted zone (p. 368)
- Step 9: Wait for DNS resolvers to start using the new hosted zone (p. 369)
- Step 10: (Optional) delete the old hosted zone (p. 369)

Step 1: Install or upgrade the AWS CLI

For information about downloading, installing, and configuring the AWS CLI, see the [AWS Command Line Interface User Guide](#).

Note

Configure the CLI so that you can use it when you're using both the account that created the hosted zone and the account that you're migrating the hosted zone to. For more information, see [Configure](#) in the *AWS Command Line Interface User Guide*

If you're already using the AWS CLI, we recommend that you upgrade to the latest version of the CLI so that the CLI commands support the latest Route 53 features.

Step 2: Create the new hosted zone

The following procedure explains how to use the Route 53 console to create the hosted zone that you want to migrate to.

Note

Route 53 assigns a new set of four name servers to the new hosted zone. After you migrate a hosted zone to another AWS account, you need to update the domain registration to use the name servers for the new hosted zone. We remind you about this step later in the process.

To create the new hosted zone using a different account

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
Sign in with the account credentials for the account that you want to migrate the hosted zone to.
2. Create a hosted zone. For more information, see [Creating a public hosted zone \(p. 340\)](#).
3. Make note of the hosted zone ID. In some cases, you'll need this information later in the process.
4. Log out of the Route 53 console.

Step 3: Create a file that contains the records that you want to migrate

To migrate records from one hosted zone to another, you create a file that contains the records that you want to migrate, edit the file, and then use the edited file to create records in the new hosted zone. Perform the following procedure to create the file.

To create a file that contains records that you want to migrate

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
Sign in with the account credentials for the account that created the hosted zone that you want to migrate.
2. Get the hosted zone ID for the hosted zone that you want to migrate:

- a. In the navigation pane, choose **Hosted zones**.
 - b. Find the hosted zone that you want to migrate. If you have a lot of hosted zones, you can choose **Exact domain name** and enter the name of the hosted zone, and press **Enter** to filter the list.
 - c. Get the value of the **Hosted zone ID** column.
3. Run the following command:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

Note the following:

- For *hosted-zone-id*, specify the ID of the hosted zone that you got in step 2 of this procedure.
- For *path-to-output-file*, specify the directory path and file name that you want to save the output in.
- The > character sends the output to the specified file.
- The AWS CLI automatically handles pagination for hosted zones that contain more than 100 records. For more information, see [Using the AWS Command Line Interface's pagination options in the AWS Command Line Interface User Guide](#).

If you use another programmatic method to list records, such as one of the AWS SDKs, you can get a maximum of 100 records per page of results. If the hosted zone contains more than 100 records, you must submit multiple requests to list all records.

- To run the command in versions of Windows PowerShell earlier than 6.0, use the following syntax:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id | Out-File path-to-output-file -Encoding utf8
```

For example, if you're running the AWS CLI on a Windows computer, you might run the following command:

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 > c:\temp\list-records-ZOLDZONE12345.txt
```

If you're running the AWS CLI on a Windows computer in a version of Windows PowerShell earlier than 6.0, you might run the following command:

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 | Out-File c:\temp\list-records-ZOLDZONE12345.txt -Encoding utf8
```

4. Make a copy of this output. After you create records in the new hosted zone, we recommend that you run the AWS CLI `list-resource-record-sets` command on the new hosted zone and compare the two outputs to ensure that all the records were created.

Step 4: Edit the records that you want to migrate

The format of the file that you created in the previous procedure is close to the format that is required by the AWS CLI `change-resource-record-sets` command that you use to create records in the new hosted zone. However, the file requires some edits. You must apply some of the changes to every record. You can make these changes using the search and replace function in a good text editor.

Open a copy of the file that you created in [Step 3: Create a file that contains the records that you want to migrate \(p. 364\)](#), and make the following changes:

- Delete the first two lines at the top of the output:

```
{  
    "ResourceRecordSets": [
```

- Delete the lines related to the NS and SOA records. The new hosted zone already has those records.
- *Optional* – Add a `Comment` element.
- Add a `Changes` element.
- For each record, add an `Action` and a `ResourceRecordSet` element.
- Add opening and closing braces ({ }) as required to make the JSON code valid.

Note

You can use a JSON validator to verify that you have all the braces and brackets in the correct places. To find an online JSON validator, do an internet search on "json validator".

- If the hosted zone contains any aliases that refer to other records in the same hosted zone, make the following changes:

- Change the hosted zone ID to the ID of the new hosted zone.

Important

If the alias record is pointing to another resource, for example, a load balancer, update the hosted zone ID to the hosted zone id of the resource itself, not the hosted zone ID of the domain. That hosted zone ID can be found from the AWS console where the resource was created.

- Move the alias records to the bottom of the file. Route 53 must create the record that an alias record refers to before it can create the alias record.

Important

If one or more alias records refer to other alias records, the records that are the alias target must appear in the file before the referencing alias records. For example, if `alias.example.com` is the alias target for `alias.alias.example.com`, `alias.example.com` must appear first in the file.

- Delete any alias records that route traffic to a traffic policy instance. Make note of the records so you can recreate them later.
- You can use this process to create records in a hosted zone that has a different name. For every record in the output, change the domain name part of the `Name` element to the name of the new hosted zone. For example, if you list records in the `example.com` hosted zone and you want to create records in an `example.net` hosted zone, change the `example.com` part of every record name to `example.net`:

From:

- "Name": "example.com."
- "Name": "www.example.com."

To:

- "Name": "example.net."
- "Name": "www.example.net."

The following example shows the edited version of records for a hosted zone for `example.com`. The red, italicized text is new:

```
{  
    "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."
    }
}
]
}

```

Step 5: Split large files into smaller files

If you have a lot of records or if you have records that have a lot of values (for example, a lot of IP addresses), you might need to split the file into smaller files. Here are the maximums:

- Each file can contain a maximum of 1,000 records.
- The maximum combined length of the values in all `Value` elements is 32,000 bytes.

Step 6: Create records in the new hosted zone

To create records in the new hosted zone, use the following AWS CLI command:

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-new-hosted-zone --change-batch file://path-to-file-that-contains-records
```

For example:

```
aws route53 change-resource-record-sets --hosted-zone-id ZNEWZONE1245 --change-batch file://c:/temp/change-records-ZNEWZONE1245.txt
```

If you deleted any alias records that route traffic to a traffic policy instance, recreate them using the Route 53 console. For more information, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

Step 7: Compare records in the old and new hosted zones

To confirm that you successfully created all of your records in the new hosted zone, we recommend that you list the records in the new hosted zone and compare the output with the list of records from the old hosted zone. To do that, perform the following procedure.

To compare records in the old and new hosted zones

1. Run the following command:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id --output json  
> path-to-output-file
```

Specify the following values:

- For *hosted-zone-id*, specify the ID of the new hosted zone.
- For *path-to-output-file*, specify the directory path and file name that you want to save the output in. Use a file name that is different from the file name that you used in [Step 3: Create a file that contains the records that you want to migrate \(p. 364\)](#). Using a different file name ensures that the new file doesn't overwrite the old file.
- The > character sends output to the specified file.

For example, if you're using a Windows computer, you might run the following command:

```
aws route53 list-resource-record-sets --hosted-zone-id ZNEWZONE67890 --output json > c:\\temp\\list-records-ZNEWZONE67890.txt
```

2. Compare the output with the output from [Step 3: Create a file that contains the records that you want to migrate \(p. 364\)](#).

Other than the values of the NS and SOA records and any changes that you made in [Step 4: Edit the records that you want to migrate \(p. 365\)](#) (such as different hosted zone IDs or domain names), the two outputs should be identical.

3. If the records in the new hosted zone don't match the records in the old hosted zone, you can do one of the following:
 - Make minor corrections using the Route 53 console. For more information, see [Editing records \(p. 440\)](#).
 - If a large number of records are missing, create a new text file that contains the missing records and then repeat [Step 6: Create records in the new hosted zone \(p. 367\)](#).
 - Delete all the records except the NS and SOA records in the new hosted zone, and repeat the following steps:
 - [Step 4: Edit the records that you want to migrate \(p. 365\)](#)
 - [Step 5: Split large files into smaller files \(p. 367\)](#)
 - [Step 6: Create records in the new hosted zone \(p. 367\)](#)
 - [Step 7: Compare records in the old and new hosted zones \(p. 368\)](#)

Step 8: Update the domain registration to use name servers for the new hosted zone

When you finish creating records in the new hosted zone, change the name servers for the domain registration to use the name servers for the new hosted zone.

Important

If you don't update the domain registration to use the name servers for the new hosted zone, Route 53 will continue to use the old hosted zone to route traffic for the domain. If you delete the old hosted zone without updating name servers for the domain registration, the domain will become unavailable on the internet. If you add, update, or delete records in the new hosted zone without updating name servers for the domain registration, then traffic won't be routed based on those changes.

For more information, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Note

Whether you use the process to migrate DNS service for a domain that's in use or the process for an inactive domain, you can skip the following steps because you've already created a new hosted zone and the records in that hosted zone:

- Step 1: Get Your Current DNS Configuration from the Current DNS Service Provider
- Step 2: Create a Hosted Zone
- Step 3: Create Records

Step 9: Wait for DNS resolvers to start using the new hosted zone

If your domain is in use—for example, if your users are using the domain name to browse to a website or access a web application—then DNS resolvers have cached the names of the name servers that were provided by your current DNS service provider. A DNS resolver that cached that information a few minutes ago will save it for up to two days.

Note

If you created any records in the new hosted zone that don't appear in the old hosted zone, your users can't use the new records to access your resources until resolvers start using the name servers for the new hosted zone. For example, suppose you create a record, test.example.com, in the new hosted zone that should route internet traffic to your website. If the record doesn't appear in the old hosted zone, you can't enter test.example.com in a web browser until resolvers start using the new hosted zone.

To ensure that migrating a hosted zone to another AWS account has completed before you delete the old hosted zone, wait for two days after you update the domain registration to use name servers for the new hosted zone. After the two-day TTL expires and resolvers request the name servers for your domain, the resolvers will get the current name servers. You can also enable [Resolver query logging \(p. 619\)](#) to monitor the queries in the new hosted zones. For information about the pricing for Resolver query logging, see [CloudWatch pricing](#).

Step 10: (Optional) delete the old hosted zone

When you're confident that you don't need the old hosted zone any longer, you can optionally delete it.

Important

Don't delete the old hosted zone or any records in that hosted zone for at least 48 hours after you update the domain registration to use name servers for the new hosted zone. If you delete the old hosted zone before DNS resolvers stop using the records in that hosted zone, your domain could be unavailable on the internet until resolvers start using the new hosted zone.

The hosted zone must be empty except for the default NS and SOA records. If the old hosted zone contains a lot of records, deleting them using the console can take a long time. One option is to perform the following steps:

1. Make another copy of the edited file from [Step 4: Edit the records that you want to migrate \(p. 365\)](#).

2. In the copy of the file, change "Action": "CREATE" to "Action": "DELETE" for every record.
3. Use the following AWS CLI command to delete the records:

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-old-hosted-zone --  
change-batch file:///path-to-file-that-contains-records
```

Important

Make sure that the value that you specify for the hosted zone ID is the ID of the old hosted zone, not the ID of the new hosted zone.

4. Delete any remaining records and the hosted zone:
 - a. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

Sign in with the account credentials for the account that created the old hosted zone.
 - b. In the navigation pane, choose **Hosted zones**.
 - c. Choose the name of the old hosted zone. If you have a lot of hosted zones, you can choose **Exact domain name** and enter the name of the hosted zone, and press **Enter** to filter the list.
 - d. If the hosted zone contains any records other than the default NS and SOA records (such as alias records that route traffic to a traffic policy instance), choose the corresponding check boxes and choose **Delete**.
 - e. In the navigation pane, choose **Hosted zones**.
 - f. In the list of hosted zones, choose the radio button for the hosted zone that you want to delete.
 - g. Choose **Delete**.

Working with records

After you create a hosted zone for your domain, such as example.com, you create records to tell the Domain Name System (DNS) how you want traffic to be routed for that domain.

For example, you might create records that cause DNS to do the following:

- Route internet traffic for example.com to the IP address of a host in your data center.
- Route email for that domain (ichiro@example.com) to a mail server (mail.example.com).
- Route traffic for a subdomain called operations.tokyo.example.com to the IP address of a different host.

Each record includes the name of a domain or a subdomain, a record type (for example, a record with a type of MX routes email), and other information applicable to the record type (for MX records, the host name of one or more mail servers and a priority for each server). For information about the different record types, see [Supported DNS record types \(p. 382\)](#).

The name of each record in a hosted zone must end with the name of the hosted zone. For example, the example.com hosted zone can contain records for www.example.com and accounting.tokyo.example.com subdomains, but cannot contain records for a www.example.ca subdomain.

Note

To create records for complex routing configurations, you can also use the traffic flow visual editor and save the configuration as a traffic policy. You can then associate the traffic policy with one or more domain names (such as example.com) or subdomain names (such as www.example.com), in the same hosted zone or in multiple hosted zones. In addition, you can roll back the updates if the new configuration isn't performing as you expected it to. For more information, see [Using traffic flow to route DNS traffic \(p. 442\)](#).

Amazon Route 53 doesn't charge for the records that you add to a hosted zone. For information about the maximum number of records that you can create in a hosted zone, see [Quotas \(p. 671\)](#).

Topics

- [Choosing a routing policy \(p. 371\)](#)
- [Choosing between alias and non-alias records \(p. 379\)](#)
- [Supported DNS record types \(p. 382\)](#)
- [Creating records by using the Amazon Route 53 console \(p. 392\)](#)
- [Values that you specify when you create or edit Amazon Route 53 records \(p. 393\)](#)
- [Creating records by importing a zone file \(p. 438\)](#)
- [Editing records \(p. 440\)](#)
- [Deleting records \(p. 440\)](#)
- [Listing records \(p. 441\)](#)

Choosing a routing policy

When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the best latency with less round-trip time.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

Topics

- [Simple routing \(p. 371\)](#)
- [Failover routing \(p. 372\)](#)
- [Geolocation routing \(p. 372\)](#)
- [Geoproximity routing \(traffic flow only\) \(p. 373\)](#)
- [Latency-based routing \(p. 377\)](#)
- [Multivalue answer routing \(p. 378\)](#)
- [Weighted routing \(p. 378\)](#)
- [How Amazon Route 53 uses EDNS0 to estimate the location of a user \(p. 379\)](#)

Simple routing

Simple routing lets you configure standard DNS records, with no special Route 53 routing such as weighted or latency. With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.

If you choose the simple routing policy in the Route 53 console, you can't create multiple records that have the same name and type, but you can specify multiple values in the same record, such as multiple IP addresses. (If you choose the simple routing policy for an alias record, you can specify only one AWS resource or one record in the current hosted zone.) If you specify multiple values in a record, Route 53 returns all values to the recursive resolver in random order, and the resolver returns the values to the client (such as a web browser) that submitted the DNS query. The client then chooses a value and resubmits the query.

For information about values that you specify when you use the simple routing policy to create records, see the following topics:

- [Values specific for simple records \(p. 402\)](#)
- [Values specific for simple alias records \(p. 404\)](#)
- [Values that are common for all routing policies \(p. 394\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)

Failover routing

Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records. For more information, see [Active-passive failover \(p. 548\)](#).

For information about values that you specify when you use the failover routing policy to create records, see the following topics:

- [Values specific for failover records \(p. 406\)](#)
- [Values specific for failover alias records \(p. 409\)](#)
- [Values that are common for all routing policies \(p. 394\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)

Geolocation routing

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.

You can specify geographic locations by continent, by country, or by state in the United States. If you create separate records for overlapping geographic regions—for example, one record for North America and one for Canada—priority goes to the smallest geographic region. This allows you to route some queries for a continent to one resource and to route queries for selected countries on that continent to a different resource. (For a list of the countries on each continent, see [Location \(p. 414\)](#).)

Geolocation works by mapping IP addresses to locations. However, some IP addresses aren't mapped to geographic locations, so even if you create geolocation records that cover all seven continents, Amazon Route 53 will receive some DNS queries from locations that it can't identify. You can create a default record that handles both queries from IP addresses that aren't mapped to any location and queries

that come from locations that you haven't created geolocation records for. If you don't create a default record, Route 53 returns a "no answer" response for queries from those locations.

For more information, see [How Amazon Route 53 uses EDNS0 to estimate the location of a user \(p. 379\)](#).

For information about values that you specify when you use the geolocation routing policy to create records, see the following topics:

- [Values specific for geolocation records \(p. 413\)](#)
- [Values specific for geolocation alias records \(p. 417\)](#)
- [Values that are common for all routing policies \(p. 394\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)

Geoproximity routing (traffic flow only)

Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a *bias*. A bias expands or shrinks the size of the geographic region from which traffic is routed to a resource.

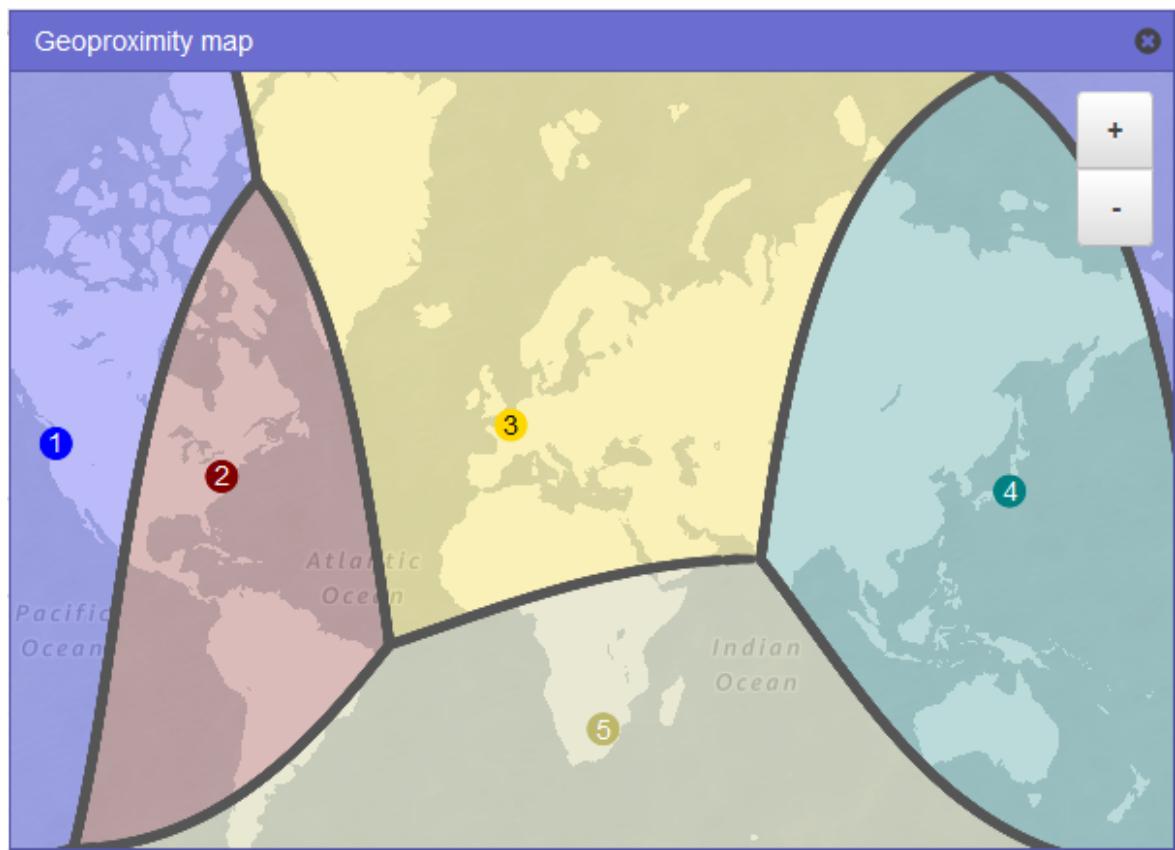
To use geoproximity routing, you must use Route 53 [traffic flow](#). You create geoproximity rules for your resources and specify one of the following values for each rule:

- If you're using AWS resources, the AWS Region that you created the resource in
- If you're using non-AWS resources, the latitude and longitude of the resource

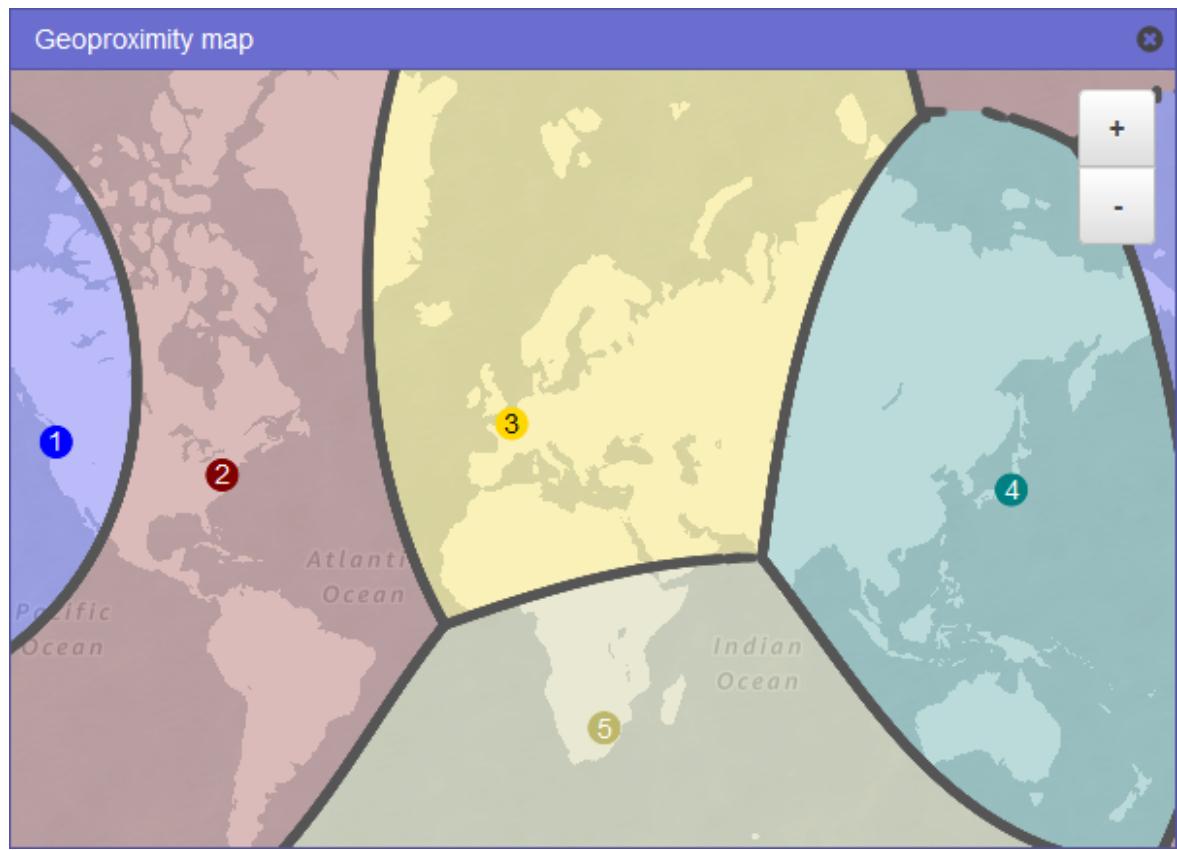
To optionally change the size of the geographic region from which Route 53 routes traffic to a resource, specify the applicable value for the bias:

- To expand the size of the geographic region from which Route 53 routes traffic to a resource, specify a positive integer from 1 to 99 for the bias. Route 53 shrinks the size of adjacent regions.
- To shrink the size of the geographic region from which Route 53 routes traffic to a resource, specify a negative bias of -1 to -99. Route 53 expands the size of adjacent regions.

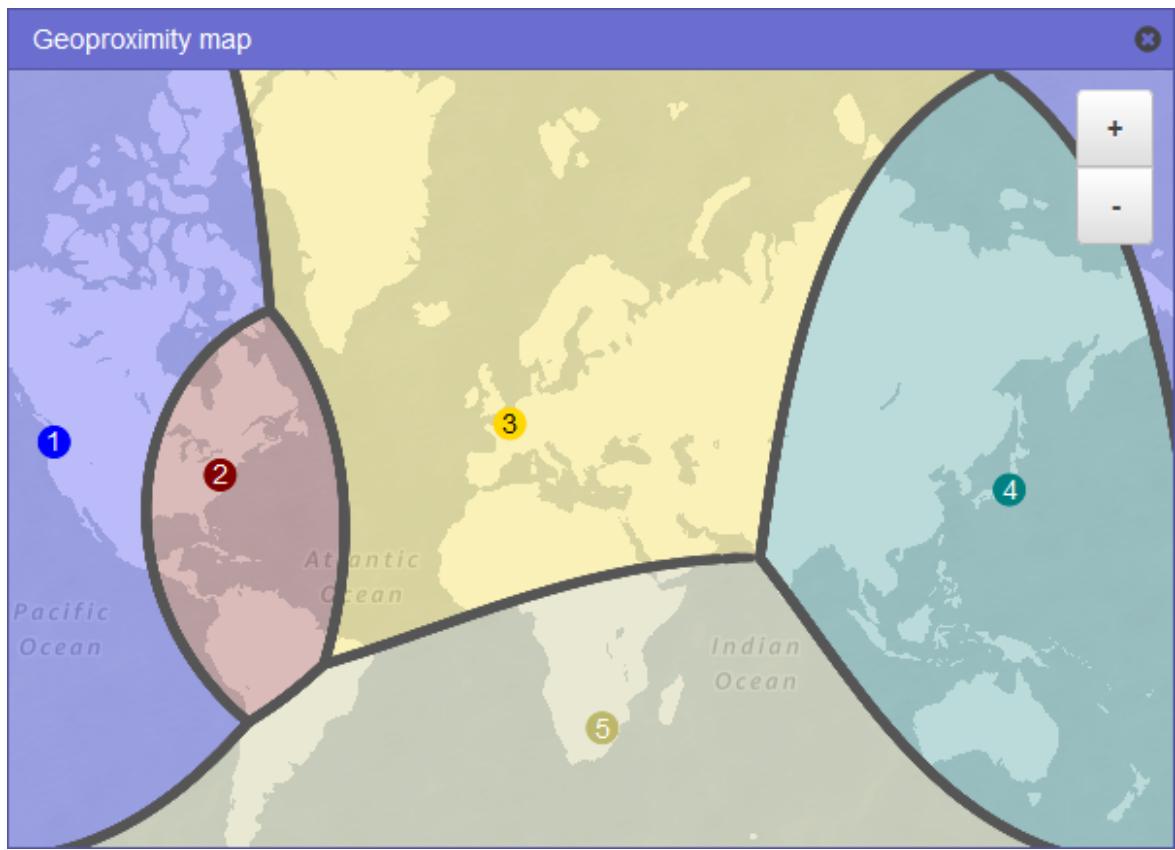
The following map shows four AWS Regions (numbered 1 through 4) and a location in Johannesburg, South Africa that is specified by latitude and longitude (5).



The following map shows what happens if you add a bias of +25 for the US East (Northern Virginia) Region (number 2 on the map). Traffic is routed to the resource in that Region from a larger portion of North America than previously, and from all of South America.



The following map shows what happens if you change the bias to -25 for the US East (Northern Virginia) Region. Traffic is routed to the resource in that Region from smaller portions of North and South America than previously, and more traffic is routed to resources in the adjacent regions **1**, **3**, and **5**.



The effect of changing the bias for your resources depends on a number of factors, including the following:

- The number of resources that you have.
- How close the resources are to one another.
- The number of users that you have near the border area between geographic regions. For example, suppose you have resources in the AWS Regions US East (Northern Virginia) and US West (Oregon) and you have a lot of users in Dallas, Austin, and San Antonio, Texas, USA. Those cities are roughly equidistant between your resources, so a small change in bias could result in a large swing in traffic from resources in one AWS Region to the other.

We recommend that you change the bias in small increments to prevent overwhelming your resources due to an unanticipated swing in traffic.

For more information, see [How Amazon Route 53 uses EDNS0 to estimate the location of a user \(p. 379\)](#).

How Amazon Route 53 uses bias to route traffic

Here's the formula that Amazon Route 53 uses to determine how to route traffic:

Positive bias

$\text{Biased distance} = \text{actual distance} * [1 - (\text{bias}/100)]$

Negative bias

$\text{Biased distance} = \text{actual distance} / [1 + (\text{bias}/100)]$

When the value of the bias is positive, Route 53 treats the source of a DNS query and the resource that you specify in a geoproximity record (such as an EC2 instance in an AWS Region) as if they were closer together than they really are. For example, suppose you have the following geoproximity records:

- A record for web server A, which has a positive bias of 50
- A record for web server B, which has no bias

When a geoproximity record has a positive bias of 50, Route 53 halves the distance between the source of a query and the resource for that record. Then Route 53 calculates which resource is closer to the source of the query. Suppose web server A is 150 kilometers from the source of a query and web server B is 100 kilometers from the source of the query. If neither record had a bias, Route 53 would route the query to web server B because it's closer. However, because the record for web server A has a positive bias of 50, Route 53 treats web server A as if it's 75 kilometers from the source of the query. As a result, Route 53 routes the query to web server A.

Here's the calculation for a positive bias of 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
```

Latency-based routing

If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.

Note

Data about the latency between users and your resources is based entirely on traffic between users and AWS data centers. If you aren't using resources in an AWS Region, the actual latency between your users and your resources can vary significantly from AWS latency data. This is true even if your resources are located in the same city as an AWS Region.

To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or acme.example.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region. Route 53 responds with the value from the selected record, such as the IP address for a web server.

For example, suppose you have ELB load balancers in the US West (Oregon) Region and in the Asia Pacific (Singapore) Region. You created a latency record for each load balancer. Here's what happens when a user in London enters the name of your domain in a browser:

1. DNS routes the query to a Route 53 name server.
2. Route 53 refers to its data on latency between London and the Singapore region and between London and the Oregon region.
3. If latency is lower between the London and Oregon regions, Route 53 responds to the query with the IP address for the Oregon load balancer. If latency is lower between London and the Singapore region, Route 53 responds with the IP address for the Singapore load balancer.

Latency between hosts on the internet can change over time as a result of changes in network connectivity and routing. Latency-based routing is based on latency measurements performed over a period of time, and the measurements reflect these changes. A request that is routed to the Oregon region this week might be routed to the Singapore region next week.

Note

When a browser or other viewer uses a DNS resolver that supports the edns-client-subnet extension of EDNS0, the DNS resolver sends Route 53 a truncated version of the user's IP address. If you configure latency-based routing, Route 53 considers this value when routing traffic to your resources. For more information, see [How Amazon Route 53 uses EDNS0 to estimate the location of a user \(p. 379\)](#).

For information about values that you specify when you use the latency routing policy to create records, see the following topics:

- [Values specific for latency records \(p. 422\)](#)
- [Values specific for latency alias records \(p. 425\)](#)
- [Values that are common for all routing policies \(p. 394\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)

Multivalue answer routing

Multivalue answer routing lets you configure Amazon Route 53 to return multiple values, such as IP addresses for your web servers, in response to DNS queries. You can specify multiple values for almost any record, but multivalue answer routing also lets you check the health of each resource, so Route 53 returns only values for healthy resources. It's not a substitute for a load balancer, but the ability to return multiple health-checkable IP addresses is a way to use DNS to improve availability and load balancing.

To route traffic approximately randomly to multiple resources, such as web servers, you create one multivalue answer record for each resource and, optionally, associate a Route 53 health check with each record. Route 53 responds to DNS queries with up to eight healthy records and gives different answers to different DNS resolvers. If a web server becomes unavailable after a resolver caches a response, client software can try another IP address in the response.

Note the following:

- If you associate a health check with a multivalue answer record, Route 53 responds to DNS queries with the corresponding IP address only when the health check is healthy.
- If you don't associate a health check with a multivalue answer record, Route 53 always considers the record to be healthy.
- If you have eight or fewer healthy records, Route 53 responds to all DNS queries with all the healthy records.
- When all records are unhealthy, Route 53 responds to DNS queries with up to eight unhealthy records.

For information about values that you specify when you use the multivalue answer routing policy to create records, see [Values specific for multivalue answer records \(p. 429\)](#) and [Values that are common for all routing policies \(p. 394\)](#).

Weighted routing

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.

To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group:

$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$

For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1/256th of the traffic ($1/(1+255)$), and the other resource gets 255/256ths ($255/(1+255)$). You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.

For information about values that you specify when you use the weighted routing policy to create records, see the following topics:

- [Values specific for weighted records \(p. 432\)](#)
- [Values specific for weighted alias records \(p. 435\)](#)
- [Values that are common for all routing policies \(p. 394\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)

How Amazon Route 53 uses EDNS0 to estimate the location of a user

To improve the accuracy of geolocation, geoproximity, and latency routing, Amazon Route 53 supports the edns-client-subnet extension of EDNS0. (EDNS0 adds several optional extensions to the DNS protocol.) Route 53 can use edns-client-subnet only when DNS resolvers support it:

- When a browser or other viewer uses a DNS resolver that does not support edns-client-subnet, Route 53 uses the source IP address of the DNS resolver to approximate the location of the user and responds to geolocation queries with the DNS record for the resolver's location.
- When a browser or other viewer uses a DNS resolver that does support edns-client-subnet, the DNS resolver sends Route 53 a truncated version of the user's IP address. Route 53 determines the location of the user based on the truncated IP address rather than the source IP address of the DNS resolver; this typically provides a more accurate estimate of the user's location. Route 53 then responds to geolocation queries with the DNS record for the user's location.

For more information about edns-client-subnet, see the IETF draft [Client Subnet in DNS Requests](#).

Choosing between alias and non-alias records

Amazon Route 53 *alias records* provide a Route 53-specific extension to DNS functionality. Alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 buckets. They also let you route traffic from one record in a hosted zone to another record.

Unlike a CNAME record, you can create an alias record at the top node of a DNS namespace, also known as the *zone apex*. For example, if you register the DNS name example.com, the zone apex is example.com. You can't create a CNAME record for example.com, but you can create an alias record for example.com that routes traffic to www.example.com (as long as www.example.com doesn't already have a CNAME record).

When Route 53 receives a DNS query for an alias record, Route 53 responds with the applicable value for that resource:

- **An Amazon API Gateway custom regional API or edge-optimized API** – Route 53 responds with one or more IP addresses for your API.
- **An Amazon VPC interface endpoint** – Route 53 responds with one or more IP addresses for your interface endpoint.

- **A CloudFront distribution** – Route 53 responds with one or more IP addresses for CloudFront edge servers that can serve your content.
- **An Elastic Beanstalk environment** – Route 53 responds with one or more IP addresses for the environment.
- **An ELB load balancer** – Route 53 responds with one or more IP addresses for the load balancer.
- **An AWS Global Accelerator accelerator** – Route 53 responds with one of the two IP addresses for the accelerator.
- **An Amazon S3 bucket that is configured as a static website** – Route 53 responds with one IP address for the Amazon S3 bucket.
- **Another Route 53 record in the same hosted zone** – Route 53 responds as if the query is for the record that is referenced by the alias record.

When you use an alias record to route traffic to an AWS resource, Route 53 automatically recognizes changes in the resource. For example, suppose an alias record for example.com points to an ELB load balancer at lb1-1234.us-east-2.elb.amazonaws.com. If the IP address of the load balancer changes, Route 53 automatically starts to respond to DNS queries using the new IP address.

If an alias record points to an AWS resource, you can't set the time to live (TTL); Route 53 uses the default TTL for the resource. If an alias record points to another record in the same hosted zone, Route 53 uses the TTL of the record that the alias record points to. For more information about the current TTL value for Elastic Load Balancing, go to [Request routing](#) in the *Elastic Load Balancing User Guide* and search for "ttl".

For information about creating records by using the Route 53 console, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#). For information about the values that you specify for alias records, see the applicable topic in [Values that you specify when you create or edit Amazon Route 53 records \(p. 393\)](#):

- [Values specific for simple alias records \(p. 404\)](#)
- [Values specific for weighted alias records \(p. 435\)](#)
- [Values specific for latency alias records \(p. 425\)](#)
- [Values specific for failover alias records \(p. 409\)](#)
- [Values specific for geolocation alias records \(p. 417\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)

Comparison of alias and CNAME records

Alias records are similar to CNAME records, but there are some important differences. The following list compares alias records and CNAME records.

Resources that you can redirect queries to

Alias records

An alias record can only redirect queries to selected AWS resources, such as the following:

- Amazon S3 buckets
- CloudFront distributions
- Another record in the same Route 53 hosted zone

For example, you can create an alias record named acme.example.com that redirects queries to an Amazon S3 bucket that is also named acme.example.com. You can also create an acme.example.com alias record that redirects queries to a record named zenith.example.com in the example.com hosted zone.

CNAME records

A CNAME record can redirect DNS queries to any DNS record. For example, you can create a CNAME record that redirects queries from acme.example.com to zenith.example.com or to acme.example.org. You don't need to use Route 53 as the DNS service for the domain that you're redirecting queries to.

Creating records that have the same name as the domain (records at the zone apex)

Alias records

In most configurations, you can create an alias record that has the same name as the hosted zone (the zone apex). The one exception is when you want to redirect queries from the zone apex (such as example.com) to a record in the same hosted zone that has a type of CNAME (such as zenith.example.com). The alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

CNAME records

You can't create a CNAME record that has the same name as the hosted zone (the zone apex). This is true both for hosted zones for domain names (example.com) and for hosted zones for subdomains (zenith.example.com).

Pricing for DNS queries

Alias records

Route 53 doesn't charge for alias queries to AWS resources. For more information, see [Amazon Route 53 Pricing](#).

CNAME records

Route 53 charges for CNAME queries.

Note

If you create a CNAME record that redirects to the name of another record in a Route 53 hosted zone (the same hosted zone or another hosted zone), each DNS query is charged as two queries:

- Route 53 responds to the first DNS query with the name of the record that you want to redirect to.
- Then the DNS resolver must submit another query for the record in the first response to get information about where to direct traffic, for example, the IP address of a web server.

If the CNAME record redirects to the name of a record that is hosted with another DNS service, Route 53 charges for one query. The other DNS service might charge for the second query.

Record type specified in the DNS query

Alias records

Route 53 responds to a DNS query only when the name of the alias record (such as acme.example.com) and the type of the alias record (such as A or AAAA) match the name and type in the DNS query.

CNAME records

A CNAME record redirects DNS queries for a record name regardless of the record type specified in the DNS query, such as A or AAAA.

How records are listed in dig or nslookup queries

Alias records

In the response to a dig or nslookup query, an alias record is listed as the record type that you specified when you created the record, such as A or AAAA. (The record type that you specify

for an alias record depends on the resource that you're routing traffic to. For example, to route traffic to an S3 bucket, you specify A for the type.) The alias property is visible only in the Route 53 console or in the response to a programmatic request, such as an AWS CLI `list-resource-record-sets` command.

CNAME records

A CNAME record is listed as a CNAME record in response to dig or nslookup queries.

Supported DNS record types

Amazon Route 53 supports the DNS record types that are listed in this section. Each record type also includes an example of how to format the `Value` element when you are accessing Route 53 using the API.

Note

For record types that include a domain name, enter a fully qualified domain name, for example, `www.example.com`. The trailing dot is optional; Route 53 assumes that the domain name is fully qualified. This means that Route 53 treats `www.example.com` (without a trailing dot) and `www.example.com.` (with a trailing dot) as identical.

Route 53 provides an extension to DNS functionality known as alias records. Similar to CNAME records, alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 buckets. For more information, including a comparison of alias and CNAME records, see [Choosing between alias and non-alias records \(p. 379\)](#).

Topics

- [A record type \(p. 382\)](#)
- [AAAA record type \(p. 383\)](#)
- [CAA record type \(p. 383\)](#)
- [CNAME record type \(p. 386\)](#)
- [DS record type \(p. 386\)](#)
- [MX record type \(p. 387\)](#)
- [NAPTR record type \(p. 387\)](#)
- [NS record type \(p. 389\)](#)
- [PTR record type \(p. 389\)](#)
- [SOA record type \(p. 389\)](#)
- [SPF record type \(p. 390\)](#)
- [SRV record type \(p. 390\)](#)
- [TXT record type \(p. 390\)](#)

A record type

You use an A record to route traffic to a resource, such as a web server, using an IPv4 address in dotted decimal notation.

Example for the Amazon Route 53 console

```
192.0.2.1
```

Example for the Route 53 API

```
<Value>192.0.2.1</Value>
```

AAAA record type

You use an AAAA record to route traffic to a resource, such as a web server, using an IPv6 address in colon-separated hexadecimal format.

Example for the Amazon Route 53 console

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Example for the Route 53 API

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

CAA record type

A CAA record specifies which certificate authorities (CAs) are allowed to issue certificates for a domain or subdomain. Creating a CAA record helps to prevent the wrong CAs from issuing certificates for your domains. A CAA record isn't a substitute for the security requirements that are specified by your certificate authority, such as the requirement to validate that you're the owner of a domain.

You can use CAA records to specify the following:

- Which certificate authorities (CAs) can issue SSL/TLS certificates, if any
- The email address or URL to contact when a CA issues a certificate for the domain or subdomain

When you add a CAA record to your hosted zone, you specify three settings separated by spaces:

```
flags tag "value"
```

Note the following about the format for CAA records:

- The value of tag can contain only the characters A-Z, a-z, and 0-9.
- Always enclose value in quotation marks ("").
- Some CAs allow or require additional values for value. Specify additional values as name-value pairs, and separate them with semicolons (;), for example:

```
0 issue "ca.example.net; account=123456"
```

- If a CA receives a request for a certificate for a subdomain (such as www.example.com) and if no CAA record for the subdomain exists, the CA submits a DNS query for a CAA record for the parent domain (such as example.com). If a record for the parent domain exists and if the certificate request is valid, the CA issues the certificate for the subdomain.
- We recommend that you consult with your CA to determine what values to specify for a CAA record.
- You can't create a CAA record and a CNAME record that have the same name because DNS doesn't allow using the same name for both a CNAME record and any other type of record.

Topics

- [Authorize a CA to issue a certificate for a domain or subdomain \(p. 384\)](#)
- [Authorize a CA to issue a wildcard certificate for a domain or subdomain \(p. 384\)](#)
- [Prevent any CA from issuing a certificate for a domain or subdomain \(p. 384\)](#)
- [Request that any CA contacts you if the CA receives an invalid certificate request \(p. 385\)](#)

- [Use another setting that is supported by the CA \(p. 385\)](#)
- [Examples \(p. 385\)](#)

Authorize a CA to issue a certificate for a domain or subdomain

To authorize a CA to issue a certificate for a domain or subdomain, create a record that has the same name as the domain or subdomain, and specify the following settings:

- **flags** – 0
- **tag** – issue
- **value** – the code for the CA that you authorize to issue a certificate for the domain or subdomain

For example, suppose you want to authorize ca.example.net to issue a certificate for example.com. You create a CAA record for example.com with the following settings:

```
0 issue "ca.example.net"
```

For information about how to authorize AWS Certificate Manager to issue a certificate, see [Configure a CAA record in the AWS Certificate Manager User Guide](#).

Authorize a CA to issue a wildcard certificate for a domain or subdomain

To authorize a CA to issue a wildcard certificate for a domain or subdomain, create a record that has the same name as the domain or subdomain, and specify the following settings. A wildcard certificate applies to the domain or subdomain and all of its subdomains.

- **flags** – 0
- **tag** – issuewild
- **value** – the code for the CA that you authorize to issue a certificate for a domain or subdomain, and its subdomains

For example, suppose you want to authorize ca.example.net to issue a wildcard certificate for example.com, which applies to example.com and all of its subdomains. You create a CAA record for example.com with the following settings:

```
0 issuewild "ca.example.net"
```

When you want to authorize a CA to issue a wildcard certificate for a domain or subdomain, create a record that has the same name as the domain or subdomain, and specify the following settings. A wildcard certificate applies to the domain or subdomain and all of its subdomains.

Prevent any CA from issuing a certificate for a domain or subdomain

To prevent any CA from issuing a certificate for a domain or subdomain, create a record that has the same name as the domain or subdomain, and specify the following settings:

- **flags** – 0
- **tag** – issue
- **value** – ";"

For example, suppose you don't want any CA to issue a certificate for example.com. You create a CAA record for example.com with the following settings:

```
0 issue ";"
```

If you don't want any CA to issue a certificate for example.com or its subdomains, you create a CAA record for example.com with the following settings:

```
0 issuewild ";"
```

Note

If you create a CAA record for example.com and specify both of the following values, a CA that is using the value ca.example.net can issue the certificate for example.com:

```
0 issue ";"  
0 issue "ca.example.net"
```

Request that any CA contacts you if the CA receives an invalid certificate request

If you want any CA that receives an invalid request for a certificate to contact you, specify the following settings:

- **flags** – 0
- **tag** – iodef
- **value** – the URL or email address that you want the CA to notify if the CA receives an invalid request for a certificate. Use the applicable format:

```
"mailto:email-address"
```

```
"http://URL"
```

```
"https://URL"
```

For example, if you want any CA that receives an invalid request for a certificate to send email to admin@example.com, you create a CAA record with the following settings:

```
0 iodef "mailto:admin@example.com"
```

Use another setting that is supported by the CA

If your CA supports a feature that isn't defined in the RFC for CAA records, specify the following settings:

- **flags** – 128 (This value prevents the CA from issuing a certificate if the CA doesn't support the specified feature.)
- **tag** – the tag that you authorize the CA to use
- **value** – the value that corresponds with the value of tag

For example, suppose your CA supports sending a text message if the CA receives an invalid certificate request. (We aren't aware of any CAs that support this option.) Settings for the record might be the following:

```
128 exAMPLetag "15555551212"
```

Examples

Example for the Route 53 console

```
0 issue "ca.example.net"
```

```
0 iodef "mailto:admin@example.com"
```

Example for the Route 53 API

```
<ResourceRecord>
  <Value>0 issue "ca.example.net"</Value>
  <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

CNAME record type

A CNAME record maps DNS queries for the name of the current record, such as acme.example.com, to another domain (example.com or example.net) or subdomain (acme.example.com or zenith.example.org).

Important

The DNS protocol does not allow you to create a CNAME record for the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You cannot create a CNAME record for example.com, but you can create CNAME records for www.example.com, newproduct.example.com, and so on.

In addition, if you create a CNAME record for a subdomain, you cannot create any other records for that subdomain. For example, if you create a CNAME for www.example.com, you cannot create any other records for which the value of the **Name** field is www.example.com.

Amazon Route 53 also supports alias records, which allow you to route queries to selected AWS resources, such as CloudFront distributions and Amazon S3 buckets. Aliases are similar in some ways to the CNAME record type; however, you can create an alias for the zone apex. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

Example for the Route 53 console

```
hostname.example.com
```

Example for the Route 53 API

```
<Value>hostname.example.com</Value>
```

DS record type

A delegation signer (DS) record refers a zone key for a delegated subdomain zone. You might create a DS record when you establish a chain of trust when you configure DNSSEC signing. For more information about configuring DNSSEC in Route 53, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

The first three values are decimal numbers representing the key tag, algorithm, and digest type. The fourth value is the digest of the zone key. For more information about the DS record format, see [RFC 4034](#).

Example for the Route 53 console

```
123 4 5 1234567890abcdef1234567890absdef
```

Example for the Route 53 API

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

MX record type

An MX record specifies the names of your mail servers and, if you have two or more mail servers, the priority order. Each value for an MX record contains two values, priority and domain name.

Priority

An integer that represents the priority for an email server. If you specify only one server, the priority can be any integer between 0 and 65535. If you specify multiple servers, the value that you specify for the priority indicates which email server you want email to be routed to first, second, and so on. The server with the lowest value for the priority takes precedence. For example, if you have two email servers and you specify values of 10 and 20 for the priority, email always goes to the server with a priority of 10 unless it's unavailable. If you specify values of 10 and 10, email is routed to the two servers approximately equally.

Domain name

The domain name of the email server. Specify the name (such as mail.example.com) of an A or AAAA record. In [RFC 2181, Clarifications to the DNS Specification](#), section 10.3 forbids specifying the name of a CNAME record for the domain name value. (When the RFC mentions "alias," it means a CNAME record, not a Route 53 alias record.)

Example for the Amazon Route 53 console

```
10 mail.example.com
```

Example for the Route 53 API

```
<Value>10 mail.example.com</Value>
```

NAPTR record type

A Name Authority Pointer (NAPTR) is a type of record that is used by Dynamic Delegation Discovery System (DDDS) applications to convert one value to another or to replace one value with another. For example, one common use is to convert phone numbers into SIP URIs.

The **Value** element for an NAPTR record consists of six space-separated values:

Order

When you specify more than one record, the sequence that you want the DDDS application to evaluate records in. Valid values: 0-65535.

Preference

When you specify two or more records that have the same **Order**, your preference for the sequence that those records are evaluated in. For example, if two records have an **Order** of 1, the DDDS application first evaluates the record that has the lower **Preference**. Valid values: 0-65535.

Flags

A setting that is specific to DDDS applications. Values currently defined in [RFC 3404](#) are uppercase-and lowercase letters "A", "P", "S", and "U", and the empty string, "". Enclose **Flags** in quotation marks.

Service

A setting that is specific to DDDS applications. Enclose **Service** in quotation marks.

For more information, see the applicable RFCs:

- **URI DDDS application** – <https://tools.ietf.org/html/rfc3404#section-4.4>
- **S-NAPTR DDDS application** – <https://tools.ietf.org/html/rfc3958#section-6.5>
- **U-NAPTR DDDS application** – <https://tools.ietf.org/html/rfc4848#section-4.5>

Regexp

A regular expression that the DDDS application uses to convert an input value into an output value. For example, an IP phone system might use a regular expression to convert a phone number that is entered by a user into a SIP URI. Enclose **Regexp** in quotation marks. Specify either a value for **Regexp** or a value for **Replacement**, but not both.

The regular expression can include any of the following printable ASCII characters:

- a-z
- 0-9
- - (hyphen)
- (space)
- ! # \$ % & ' () * + , - / ; < = > ? @ [] ^ _ ` { | } ~ .
- " (quotation mark). To include a literal quote in a string, precede it with a \ character: \".
- \ (backslash). To include a backslash in a string, precede it with a \ character: \\.

Specify all other values, such as internationalized domain names, in octal format.

For the syntax for **Regexp**, see [RFC 3402, section 3.2, Substitution Expression Syntax](#)

Replacement

The fully qualified domain name (FQDN) of the next domain name that you want the DDDS application to submit a DNS query for. The DDDS application replaces the input value with the value that you specify for **Replacement**, if any. Specify either a value for **Regexp** or a value for **Replacement**, but not both. If you specify a value for **Regexp**, specify a dot (.) for **Replacement**.

The domain name can include a-z, 0-9, and - (hyphen).

For more information about DDDS applications and about NAPTR records, see the following RFCs:

- [RFC 3401](#)
- [RFC 3402](#)
- [RFC 3403](#)
- [RFC 3404](#)

Example for the Amazon Route 53 console

```
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!" .
```

Example for the Route 53 API

```
<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>
```

NS record type

An NS record identifies the name servers for the hosted zone. Note the following:

- The most common use for an NS record is to control how internet traffic is routed for a domain. To use the records in a hosted zone to route traffic for a domain, you update the domain registration settings to use the four name servers in the default NS record. (This is the NS record that has the same name as the hosted zone.)
- You can create a separate hosted zone for a subdomain (acme.example.com) and use that hosted zone to route internet traffic for the subdomain and its subdomains (subdomain.acme.example.com). You set up this configuration, known as "delegating responsibility for a subdomain to a hosted zone" by creating another NS record in the hosted zone for the root domain (example.com). For more information, see [Routing traffic for subdomains \(p. 335\)](#).
- You also use NS records to configure white-label name servers. For more information, see [Configuring white-label name servers \(p. 349\)](#).

For more information about NS records, see [NS and SOA records that Amazon Route 53 creates for a public hosted zone \(p. 354\)](#).

Example for the Amazon Route 53 console

```
ns-1.example.com
```

Example for the Route 53 API

```
<Value>ns-1.example.com</Value>
```

PTR record type

A PTR record maps an IP address to the corresponding domain name.

Example for the Amazon Route 53 console

```
hostname.example.com
```

Example for the Route 53 API

```
<Value>hostname.example.com</Value>
```

SOA record type

A start of authority (SOA) record provides information about a domain and the corresponding Amazon Route 53 hosted zone. For information about the fields in an SOA record, see [NS and SOA records that Amazon Route 53 creates for a public hosted zone \(p. 354\)](#).

Example for the Route 53 API

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Example for the Route 53 API

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

SPF record type

SPF records were formerly used to verify the identity of the sender of email messages. However, we no longer recommend that you create records for which the record type is SPF. RFC 7208, *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1*, has been updated to say, "...[I]ts existence and mechanism defined in [RFC4408] have led to some interoperability issues. Accordingly, its use is no longer appropriate for SPF version 1; implementations are not to use it." In RFC 7208, see section 14.1, [The SPF DNS Record Type](#).

Instead of an SPF record, we recommend that you create a TXT record that contains the applicable value. For more information about valid values, see the Wikipedia article [Sender Policy Framework](#).

Example for the Amazon Route 53 console

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Example for the Route 53 API

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

SRV record type

An SRV record Value element consists of four space-separated values. The first three values are decimal numbers representing priority, weight, and port. The fourth value is a domain name. SRV records are used for accessing services, such as a service for email or communications. For information about SRV record format, refer to the documentation for the service that you want to connect to.

Example for the Amazon Route 53 console

```
10 5 80 hostname.example.com
```

Example for the Route 53 API

```
<Value>10 5 80 hostname.example.com</Value>
```

TXT record type

A TXT record contains one or more strings that are enclosed in double quotation marks (""). When you use the simple [routing policy](#), include all values for a domain (example.com) or subdomain (www.example.com) in the same TXT record.

Topics

- [Entering TXT record values \(p. 390\)](#)
- [Special characters in a TXT record value \(p. 391\)](#)
- [Uppercase and lowercase in a TXT record value \(p. 391\)](#)
- [Examples \(p. 391\)](#)

Entering TXT record values

A single string can include up to 255 characters, including the following:

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

If you need to enter a value longer than 255 characters, break the value into strings of 255 characters or fewer, and enclose each string in double quotation marks (""). In the console, list all the strings on the same line:

```
"String 1" "String 2" "String 3"
```

For the API, include all the strings in the same `Value` element:

```
<Value>"String 1" "String 2" "String 3"</Value>
```

The maximum length of a value in a TXT record is 4,000 characters.

To enter more than one TXT value, enter one value per row.

Special characters in a TXT record value

If your TXT record contains any of the following characters, you must specify the characters by using escape codes in the format `\three-digit octal code`:

- Characters 000 to 040 octal (0 to 32 decimal, 0x00 to 0x20 hexadecimal)
- Characters 177 to 377 octal (127 to 255 decimal, 0x7F to 0xFF hexadecimal)

For example, if the value of your TXT record is "exämpel.com", you specify "ex\344mple.com".

For a mapping between ASCII characters and octal codes, perform an internet search for "ascii octal codes." One useful reference is [ASCII Code - The extended ASCII table](#).

To include a quotation mark (") in a string, put a backslash (\) character before the quotation mark: \".

Uppercase and lowercase in a TXT record value

Case is preserved, so "Ab" and "aB" are different values.

Examples

Example for the Amazon Route 53 console

Put each value on a separate line:

```
"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"
```

Example for the Route 53 API

Put each value in a separate `Value` element:

```
<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>
```

Creating records by using the Amazon Route 53 console

The following procedure explains how to create records using the Amazon Route 53 console. For information about how to create records using the Route 53 API, see [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

Note

To create records for complex routing configurations, you can also use the traffic flow visual editor and save the configuration as a traffic policy. You can then associate the traffic policy with one or more domain names (such as example.com) or subdomain names (such as www.example.com), in the same hosted zone or in multiple hosted zones. In addition, you can roll back the updates if the new configuration isn't performing as you expected it to. For more information, see [Using traffic flow to route DNS traffic \(p. 442\)](#).

To create a record using the Route 53 console

1. If you're not creating an alias record, go to step 2.

Also go to step 2 if you're creating an alias record that routes DNS traffic to an AWS resource other than an Elastic Load Balancing load balancer or another Route 53 record.

If you're creating an alias record that routes traffic to an ELB load balancer, and if you created your hosted zone and your load balancer using different accounts, perform the procedure [Getting the DNS name for an ELB load balancer \(p. 393\)](#) to get the DNS name for the load balancer.

2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Hosted zones**.
4. If you already have a hosted zone for your domain, skip to step 5. If you don't, perform the applicable procedure to create a hosted zone:
 - To route internet traffic to your resources, such as Amazon S3 buckets or Amazon EC2 instances, see [Creating a public hosted zone \(p. 340\)](#).
 - To route traffic in your VPC, see [Creating a private hosted zone \(p. 359\)](#).
5. On the **Hosted zones** page, choose the name of the hosted zone that you want to create records in.
6. Choose **Create record**.
7. Choose and define the applicable routing policy and values. For more information, see the topic for the kind of record that you want to create:
 - [Values that are common for all routing policies \(p. 394\)](#)
 - [Values that are common for alias records for all routing policies \(p. 397\)](#)
 - [Values specific for simple records \(p. 402\)](#)
 - [Values specific for simple alias records \(p. 404\)](#)
 - [Values specific for failover records \(p. 406\)](#)
 - [Values specific for failover alias records \(p. 409\)](#)
 - [Values specific for geolocation records \(p. 413\)](#)
 - [Values specific for geolocation alias records \(p. 417\)](#)
 - [Values specific for latency records \(p. 422\)](#)

- [Values specific for latency alias records \(p. 425\)](#)
 - [Values specific for multivalue answer records \(p. 429\)](#)
 - [Values specific for weighted records \(p. 432\)](#)
 - [Values specific for weighted alias records \(p. 435\)](#)
8. Choose **Create records**.
- Note**
Your new records take time to propagate to the Route 53 DNS servers. Currently, the only way to verify that changes have propagated is to use the [GetChange](#) API action. Changes generally propagate to all Route 53 name servers within 60 seconds.
9. If you're creating multiple records, repeat steps 7 through 8.

Getting the DNS name for an ELB load balancer

1. Sign in to the AWS Management Console using the AWS account that was used to create the Classic, Application, or Network Load Balancer that you want to create an alias record for.
2. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
3. In the navigation pane, choose **Load Balancers**.
4. In the list of load balancers, select the load balancer for which you want to create an alias record.
5. On the **Description** tab, get the value of **DNS name**.
6. If you want to create alias records for other ELB load balancers, repeat steps 4 and 5.
7. Sign out of the AWS Management Console.
8. Sign in to the AWS Management Console again using the AWS account that you used to create the Route 53 hosted zone.
9. Return to step 3 of the procedure [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

Values that you specify when you create or edit Amazon Route 53 records

When you create records using the Amazon Route 53 console, the values that you specify depend on the routing policy that you want to use and on whether you're creating alias records, which route traffic to AWS resources.

Topics

- [Values that are common for all routing policies \(p. 394\)](#)
- [Values that are common for alias records for all routing policies \(p. 397\)](#)
- [Values specific for simple records \(p. 402\)](#)
- [Values specific for simple alias records \(p. 404\)](#)
- [Values specific for failover records \(p. 406\)](#)
- [Values specific for failover alias records \(p. 409\)](#)
- [Values specific for geolocation records \(p. 413\)](#)
- [Values specific for geolocation alias records \(p. 417\)](#)
- [Values specific for latency records \(p. 422\)](#)
- [Values specific for latency alias records \(p. 425\)](#)
- [Values specific for multivalue answer records \(p. 429\)](#)
- [Values specific for weighted records \(p. 432\)](#)
- [Values specific for weighted alias records \(p. 435\)](#)

Values that are common for all routing policies

These are the common values that you can specify when you create or edit Amazon Route 53 records. These values are used by all routing policies.

Topics

- [Record name \(p. 394\)](#)
- [Value/Route traffic to \(p. 394\)](#)
- [TTL \(seconds\) \(p. 395\)](#)

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Name** field.

CNAME records

If you're creating a record that has a value of **CNAME** for **Record type**, the name of the record can't be the same as the name of the hosted zone.

Special characters

For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).

Wildcard characters

You can use an asterisk (*) character in the name. DNS treats the * character either as a wildcard or as the * character (ASCII 42), depending on where it appears in the name. For more information, see [Using an asterisk \(*\) in the names of hosted zones and records \(p. 39\)](#).

Important

You can't use the * wildcard for resource records sets that have a type of **NS**.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. For all types except **CNAME**, you can enter more than one value. Enter each value on a separate line.

A — IPv4 address

An IP address in IPv4 format, for example, **192.0.2.235**.

AAAA — IPv6 address

An IP address in IPv6 format, for example, **2001:0db8:85a3:0:0:8a2e:0370:7334**.

CAA — Certificate Authority Authorization

Three space-separated values that control which certificate authorities are allowed to issue certificates or wildcard certificates for the domain or subdomain that is specified by **Record name**. You can use CAA records to specify the following:

- Which certificate authorities (CAs) can issue SSL/TLS certificates, if any
- The email address or URL to contact when a CA issues a certificate for the domain or subdomain

CNAME — Canonical name

The fully qualified domain name (for example, `www.example.com`) that you want Route 53 to return in response to DNS queries for this record. A trailing dot is optional; Route 53 assumes that the domain name is fully qualified. This means that Route 53 treats `www.example.com` (without a trailing dot) and `www.example.com.` (with a trailing dot) as identical.

MX — Mail exchange

A priority and a domain name that specifies a mail server, for example, **10 mailserver.example.com**. The trailing dot is treated as optional.

NAPTR — Name Authority Pointer

Six space-separated settings that are used by Dynamic Delegation Discovery System (DDDS) applications to convert one value to another or to replace one value with another. For more information, see [NAPTR record type \(p. 387\)](#).

PTR — Pointer

The domain name that you want Route 53 to return.

NS — Name server

The domain name of a name server, for example, **ns1.example.com**.

Note

You can specify an NS record with only simple routing policy.

SPF — Sender Policy Framework

An SPF record enclosed in quotation marks, for example, "`v=spf1 ip4:192.168.0.1/16-all`". SPF records are not recommended. For more information, see [Supported DNS record types \(p. 382\)](#).

SRV — Service locator

An SRV record. SRV records are used for accessing services, such as a service for email or communications. For information about SRV record format, refer to the documentation for the service that you want to connect to. Trailing dot is treated as optional.

The format of an SRV record is:

[priority] [weight] [port] [server host name]

For example:

1 10 5269 xmpp-server.example.com.

TXT — Text

A text record. Enclose text in quotation marks, for example, "**Sample text entry**".

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

If you're associating this record with a health check, we recommend that you specify a TTL of 60 seconds or less so clients respond quickly to changes in health status.

Values that are common for alias records for all routing policies

These are the common alias values that you can specify when you create or edit Amazon Route 53 records. These values are used by all routing policies.

Topics

- [Record name \(p. 397\)](#)
- [Value/route traffic to \(p. 397\)](#)

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Name** field.

CNAME records

If you're creating a record that has a value of **CNAME** for **Type**, the name of the record can't be the same as the name of the hosted zone.

Aliases to CloudFront distributions and Amazon S3 buckets

The value that you specify depends in part on the AWS resource that you're routing traffic to:

- **CloudFront distribution** – Your distribution must include an alternate domain name that matches the name of the record. For example, if the name of the record is **acme.example.com**, your CloudFront distribution must include **acme.example.com** as one of the alternate domain names. For more information, see [Using alternate domain names \(CNAMEs\)](#) in the *Amazon CloudFront Developer Guide*.
- **Amazon S3 bucket** – The name of the record must match the name of your Amazon S3 bucket. For example, if the name of your bucket is **acme.example.com**, the name of this record must also be **acme.example.com**.

In addition, you must configure the bucket for website hosting. For more information, see [Configure a bucket for website hosting](#) in the *Amazon Simple Storage Service User Guide*.

Special characters

For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see [DNS domain name format \(p. 38\)](#).

Wildcard characters

You can use an asterisk (*) character in the name. DNS treats the * character either as a wildcard or as the * character (ASCII 42), depending on where it appears in the name. For more information, see [Using an asterisk \(*\) in the names of hosted zones and records \(p. 39\)](#).

Value/route traffic to

The value that you choose from the list or that you type in the field depends on the AWS resource that you're routing traffic to.

For more information about how to configure Route 53 to route traffic to specific AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Important

If you used the same AWS account to create your hosted zone and the resource that you're routing traffic to, and if your resource doesn't appear in the **Endpoint** list, check the following:

- Confirm that you chose a supported value for **Record type**. Supported values are specific to the resource that you're routing traffic to. For example, to route traffic to an S3 bucket, you must choose **A — IPv4 address** for **Record type**.
- Confirm that the account has the IAM permissions that are required to list the applicable resources. For example, for CloudFront distributions to appear in the **Endpoint** list, the account must have permission to perform the following action: `cloudfront>ListDistributions`.

For an example IAM policy, see [Permissions required to use the Amazon Route 53 console \(p. 580\)](#).

If you used different AWS accounts to create the hosted zone and the resource, the **Endpoint** list doesn't display your resource. See the following documentation for your resource type to determine what value to type in **Endpoint**.

API Gateway custom regional APIs and edge-optimized APIs

For API Gateway custom regional APIs and edge-optimized APIs, do one of the following:

- **If you used the same account to create your Route 53 hosted zone and your API** – Choose **Endpoint**, and then choose an API from the list. If you have a lot of APIs, you can enter the first few characters of the API endpoint to filter the list.

Note

The name of this record must match a custom domain name for your API, such as `api.example.com`.

- **If you used different accounts to create your Route 53 hosted zone and your API** – Enter the API endpoint for the API, such as `api.example.com`.

If you used one AWS account to create the current hosted zone and a different account to create an API, the API won't appear in the **Endpoints** list under **API Gateway APIs**.

If you used one account to create the current hosted zone and one or more different accounts to create all of your APIs, the **Endpoints** list shows **No targets available** under **API Gateway APIs**. For more information, see [Routing traffic to an Amazon API Gateway API by using your domain name \(p. 496\)](#).

CloudFront distributions

For CloudFront distributions, do one of the following:

- **If you used the same account to create your Route 53 hosted zone and your CloudFront distribution** – Choose **Endpoint** and choose a distribution from the list. If you have a lot of distributions, you can enter the first few characters of the domain name for your distribution to filter the list.

If your distribution doesn't appear in the list, note the following:

- The name of this record must match an alternate domain name in your distribution.
 - If you just added an alternate domain name to your distribution, it may take 15 minutes for your changes to propagate to all CloudFront edge locations. Until changes have propagated, Route 53 can't know about the new alternate domain name.
- **If you used different accounts to create your Route 53 hosted zone and your distribution** – Enter the CloudFront domain name for the distribution, such as `d111111abcdef8.cloudfront.net`.

If you used one AWS account to create the current hosted zone and a different account to create a distribution, the distribution will not appear in the **Endpoints** list.

If you used one account to create the current hosted zone and one or more different accounts to create all of your distributions, the **Endpoints** list shows **No targets available** under **CloudFront distributions**.

Important

Do not route queries to a CloudFront distribution that has not propagated to all edge locations, or your users won't be able to access the applicable content.

Your CloudFront distribution must include an alternate domain name that matches the name of the record. For example, if the name of the record is **acme.example.com**, your CloudFront distribution must include **acme.example.com** as one of the alternate domain names. For more information, see [Using alternate domain names \(CNAMEs\) in the Amazon CloudFront Developer Guide](#).

If IPv6 is enabled for the distribution, create two records, one with a value of **A — IPv4 address** for **Record type**, and one with a value of **AAAA — IPv6 address**. For more information, see [Routing traffic to an Amazon CloudFront distribution by using your domain name \(p. 498\)](#).

Elastic Beanstalk environments that have regionalized subdomains

If the domain name for your Elastic Beanstalk environment includes the Region that you deployed the environment in, you can create an alias record that routes traffic to the environment. For example, the domain name **my-environment.us-west-2.elasticbeanstalk.com** is a regionalized domain name.

Important

For environments that were created before early 2016, the domain name doesn't include the Region. To route traffic to these environments, you must create a CNAME record instead of an alias record. Note that you can't create a CNAME record for the root domain name. For example, if your domain name is **example.com**, you can create a record that routes traffic for **acme.example.com** to your Elastic Beanstalk environment, but you can't create a record that routes traffic for **example.com** to your Elastic Beanstalk environment.

For Elastic Beanstalk environments that have regionalized subdomains, do one of the following:

- **If you used the same account to create your Route 53 hosted zone and your Elastic Beanstalk environment** – Choose **Endpoint**, and then choose an environment from the list. If you have a lot of environments, you can enter the first few characters of the CNAME attribute for the environment to filter the list.
- **If you used different accounts to create your Route 53 hosted zone and your Elastic Beanstalk environment** – Enter the CNAME attribute for the Elastic Beanstalk environment.

For more information, see [Routing traffic to an AWS Elastic Beanstalk environment \(p. 502\)](#).

ELB Load Balancers

For ELB load balancers, do one of the following:

- **If you used the same account to create your Route 53 hosted zone and your load balancer** – Choose **Endpoint** and choose a load balancer from the list. If you have a lot of load balancers, you can enter the first few characters of the DNS name to filter the list.
- **If you used different accounts to create your Route 53 hosted zone and your load balancer** – Enter the value that you got in the procedure [Getting the DNS name for an ELB load balancer \(p. 393\)](#).

If you used one AWS account to create the current hosted zone and a different account to create a load balancer, the load balancer will not appear in the **Endpoints** list.

If you used one account to create the current hosted zone and one or more different accounts to create all of your load balancers, the **Endpoints** list shows **No targets available** under **Elastic Load Balancers**.

The console prepends **dualstack.** for Application and Classic Load Balancer from a different account. When a client, such as a web browser, requests the IP address for your domain name (**example.com**) or subdomain name (**www.example.com**), the client can request an IPv4 address (an A record), an

IPv6 address (a AAAA record), or both IPv4 and IPv6 addresses (in separate requests). The **dualstack** designation allows Route 53 to respond with the appropriate IP address for your load balancer based on which IP address format the client requested.

For more information, see [Routing traffic to an ELB load balancer \(p. 505\)](#).

AWS Global Accelerator accelerators

For AWS Global Accelerator accelerators, enter the DNS name for the accelerator. You can enter the DNS name of an accelerator that you created using the current AWS account or using a different AWS account.

Amazon S3 Buckets

For Amazon S3 buckets that are configured as website endpoints, do one of the following:

- **If you used the same account to create your Route 53 hosted zone and your Amazon S3 bucket**
– Choose **Endpoint** and choose a bucket from the list. If you have a lot of buckets, you can enter the first few characters of the DNS name to filter the list.

The value of **Endpoint** changes to the Amazon S3 website endpoint for your bucket.

- **If you used different accounts to create your Route 53 hosted zone and your Amazon S3 bucket**
– Enter the name of the Region that you created your S3 bucket in. Use the value that appears in the **Website endpoint** column in the table [Amazon S3 website endpoints](#) in the *Amazon Web Services General Reference*.

If you used AWS accounts other than the current account to create your Amazon S3 buckets, the bucket won't appear in the **Endpoints** list.

You must configure the bucket for website hosting. For more information, see [Configure a bucket for website hosting](#) in the *Amazon Simple Storage Service User Guide*.

The name of the record must match the name of your Amazon S3 bucket. For example, if the name of your Amazon S3 bucket is **acme.example.com**, the name of this record must also be **acme.example.com**.

In a group of weighted alias, latency alias, failover alias, or geolocation alias records, you can create only one record that routes queries to an Amazon S3 bucket because the name of the record must match the name of the bucket and bucket names must be globally unique.

Amazon VPC interface endpoints

For Amazon VPC interface endpoints, do one of the following:

- **If you used the same account to create your Route 53 hosted zone and your interface endpoint**
– Choose **Endpoint**, and then choose an interface endpoint from the list. If you have a lot of interface endpoints, you can enter the first few characters of the DNS hostname to filter the list.
- **If you used different accounts to create your Route 53 hosted zone and your interface endpoint**
– Enter the DNS hostname for the interface endpoint, such as **vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com**.

If you used one AWS account to create the current hosted zone and a different account to create an interface endpoint, the interface endpoint won't appear in the **Endpoint** list under **VPC endpoints**.

If you used one account to create the current hosted zone and one or more different accounts to create all of your interface endpoints, the **Endpoint** list shows **No targets available** under **VPC endpoints**.

For more information, see [Routing traffic to an Amazon Virtual Private Cloud interface endpoint by using your domain name \(p. 509\)](#).

Records in this Hosted Zone

For records in this hosted zone, choose **Endpoint** and choose the applicable record. If you have a lot of records, you can enter the first few characters of the name to filter the list.

If the hosted zone contains only the default NS and SOA records, the **Endpoints** list shows **No targets available**.

Note

If you're creating an alias record that has the same name as the hosted zone (known as the *zone apex*), you can't choose a record for which the value of **Record type** is **CNAME**. This is because the alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

Values specific for simple records

When you create simple records, you specify the following values.

Topics

- [Routing policy \(p. 402\)](#)
- [Record name \(p. 402\)](#)
- [Value/Route traffic to \(p. 402\)](#)
- [Record type \(p. 403\)](#)
- [TTL \(seconds\) \(p. 403\)](#)

Routing policy

Choose **Simple routing**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Name** field.

For more information about record names, see [Record name \(p. 394\)](#).

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. For all types except **CNAME**, you can enter more than one value. Enter each value on a separate line.

You can route traffic to, or specify the following values:

- **A — IPv4 address**
- **AAAA — IPv6 address**
- **CAA — Certificate Authority Authorization**
- **CNAME — Canonical name**
- **MX — Mail exchange**
- **NAPTR — Name Authority Pointer**
- **NS — Name server**

The domain name of a name server, for example, **ns1.example.com**.

Note

You can specify an NS record with only simple routing policy.

- **PTR — Pointer**
- **SPF — Sender Policy Framework**
- **SRV — Service locator**
- **TXT — Text**

For more information about the above values, see [Value/Route traffic to \(p. 394\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the value for **Record type** based on how you want Route 53 to respond to DNS queries.

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

Values specific for simple alias records

When you create alias records, you specify the following values. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

Note

If you are using Route 53 in the AWS GovCloud (US) Region, this feature has some restrictions. For more information, see the [Amazon Route 53 page](#) in the *AWS GovCloud (US) User Guide*.

Topics

- [Routing policy \(p. 404\)](#)
- [Record name \(p. 404\)](#)
- [Value/route traffic to \(p. 404\)](#)
- [Record type \(p. 404\)](#)
- [Evaluate target health \(p. 405\)](#)

Routing policy

Choose **Simple routing**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Name** field.

For more information about record names, see [Record name \(p. 397\)](#).

Value/route traffic to

The value that you choose from the list or that you type in the field depends on the AWS resource that you're routing traffic to.

For information about what AWS resources you can target, see [Value/route traffic to \(p. 397\)](#).

For more information about how to configure Route 53 to route traffic to specific AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the applicable value based on the AWS resource that you're routing traffic to:

API Gateway custom regional API or edge-optimized API

Select **A — IPv4 address**.

Amazon VPC interface endpoints

Select **A — IPv4 address**.

CloudFront distribution

Select **A — IPv4 address**.

If IPv6 is enabled for the distribution, create two records, one with a value of **A — IPv4 address** for **Type**, and one with a value of **AAAA — IPv6 address**.

Elastic Beanstalk environment that has regionalized subdomains

Select **A — IPv4 address**

ELB load balancer

Select **A — IPv4 address or AAAA — IPv6 address**

Amazon S3 bucket

Select **A — IPv4 address**

Another record in this hosted zone

Select the type of the record that you're creating the alias for. All types are supported except **NS** and **SOA**.

Note

If you're creating an alias record that has the same name as the hosted zone (known as the *zone apex*), you can't route traffic to a record for which the value of **Type** is **CNAME**. This is because the alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

Evaluate target health

When the value of **Routing policy** is **Simple**, you can choose either **No** or the default **Yes** because **Evaluate target health** has no effect for **Simple** routing. If you have only one record that has a given name and type, Route 53 responds to DNS queries by using the values in that record regardless of whether the resource is healthy.

Values specific for failover records

When you create failover records, you specify the following values.

Note

For information about creating failover records in a private hosted zone, see [Configuring failover in a private hosted zone \(p. 550\)](#).

Topics

- [Routing policy \(p. 406\)](#)
- [Record name \(p. 406\)](#)
- [Record type \(p. 406\)](#)
- [TTL \(seconds\) \(p. 406\)](#)
- [Value/Route traffic to \(p. 407\)](#)
- [Failover record type \(p. 407\)](#)
- [Health check \(p. 407\)](#)
- [Record ID \(p. 408\)](#)

Routing policy

Choose **Failover**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for both of the records in the group of failover records.

For more information about record names, see [Record name \(p. 394\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the same value for both the primary and secondary failover records.

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

If you're associating this record with a health check, we recommend that you specify a TTL of 60 seconds or less so clients respond quickly to changes in health status.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. For all types except **CNAME**, you can enter more than one value. Enter each value on a separate line.

You can route traffic to, or specify the following values:

- **A — IPv4 address**
- **AAAA — IPv6 address**
- **CAA — Certificate Authority Authorization**
- **CNAME — Canonical name**
- **MX — Mail exchange**
- **NAPTR — Name Authority Pointer**
- **PTR — Pointer**
- **SPF — Sender Policy Framework**
- **SRV — Service locator**
- **TXT — Text**

For more information about the above values, see [Value/Route traffic to \(p. 394\)](#).

Failover record type

Choose the applicable value for this record. For failover to function correctly, you must create one primary and one secondary failover record.

You can't create non-failover records that have the same values for **Record name** and **Record type** as failover records.

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate Target Health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is

serving content for www.example.com. For the value of **Domain Name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain Name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Record ID

Enter a value that uniquely identifies the primary and secondary records.

Values specific for failover alias records

When you create failover alias records, you specify the following values.

For information, see the following topics:

- For information about creating failover records in a private hosted zone, see [Configuring failover in a private hosted zone \(p. 550\)](#).
- For information about alias records, see [Choosing between alias and non-alias records \(p. 379\)](#).

Topics

- [Routing policy \(p. 409\)](#)
- [Record name \(p. 409\)](#)
- [Record type \(p. 409\)](#)
- [Value/Route traffic to \(p. 410\)](#)
- [Failover record type \(p. 410\)](#)
- [Health check \(p. 410\)](#)
- [Evaluate target health \(p. 411\)](#)
- [Record ID \(p. 412\)](#)

Routing policy

Choose **Failover**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for both of the records in the group of failover records.

For more information about record names, see [Record name \(p. 397\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the applicable value based on the AWS resource that you're routing traffic to. Select the same value for both the primary and secondary failover records:

API Gateway custom regional API or edge-optimized API

Select **A — IPv4 address**.

Amazon VPC interface endpoints

Select **A — IPv4 address**.

CloudFront distribution

Select **A — IPv4 address**.

If IPv6 is enabled for the distribution, create two records, one with a value of **A — IPv4 address** for **Type**, and one with a value of **AAAA — IPv6 address**.

Elastic Beanstalk environment that has regionalized subdomains

Select **A — IPv4 address**

ELB load balancer

Select **A — IPv4 address or AAAA — IPv6 address**

Amazon S3 bucket

Select **A — IPv4 address**

Another record in this hosted zone

Select the type of the record that you're creating the alias for. All types are supported except **NS** and **SOA**.

Note

If you're creating an alias record that has the same name as the hosted zone (known as the *zone apex*), you can't route traffic to a record for which the value of **Type** is **CNAME**. This is because the alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

Value/Route traffic to

The value that you choose from the list or that you type in the field depends on the AWS resource that you're routing traffic to.

For information about what AWS resources you can target, see [Value/route traffic to \(p. 397\)](#).

For more information about how to configure Route 53 to route traffic to specific AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Note

When you create primary and secondary failover records, you can optionally create one failover and one failover *alias* record that have the same values for **Name** and **Record type**. If you mix failover and failover alias records, either one can be the primary record.

Failover record type

Choose the applicable value for this record. For failover to function correctly, you must create one primary and one secondary failover record.

You can't create non-failover records that have the same values for **Record name** and **Record type** as failover records.

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate Target Health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain Name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain Name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Evaluate target health

Select **Yes** if you want Route 53 to determine whether to respond to DNS queries using this record by checking the health of the resource specified by **Endpoint**.

Note the following:

API Gateway custom regional APIs and edge-optimized APIs

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an API Gateway custom regional API or an edge-optimized API.

CloudFront distributions

You can't set **Evaluate target health** to **Yes** when the endpoint is a CloudFront distribution.

Elastic Beanstalk environments that have regionalized subdomains

If you specify an Elastic Beanstalk environment in **Endpoint** and the environment contains an ELB load balancer, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. (An environment automatically contains an ELB load balancer if it includes more than one Amazon EC2 instance.) If you set **Evaluate target health** to **Yes** and either no Amazon EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other available resources that are healthy, if any.

If the environment contains a single Amazon EC2 instance, there are no special requirements.

ELB load balancers

Health checking behavior depends on the type of load balancer:

- **Classic load balancers** – If you specify an ELB Classic Load Balancer in **Endpoint**, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. If you set **Evaluate target health** to **Yes** and either no EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other resources.
- **Application and Network Load Balancers** – If you specify an ELB Application or Network Load Balancer and you set **Evaluate Target health** to **Yes**, Route 53 routes queries to the load balancer based on the health of the target groups that are associated with the load balancer:
 - For an Application or Network Load Balancer to be considered healthy, every target group that contains targets must contain at least one healthy target. If any target group contains only unhealthy targets, the load balancer is considered unhealthy, and Route 53 routes queries to other resources.

- A target group that has no registered targets is considered unhealthy.

Note

When you create a load balancer, you configure settings for Elastic Load Balancing health checks; they're not Route 53 health checks, but they perform a similar function. Do not create Route 53 health checks for the EC2 instances that you register with an ELB load balancer.

S3 buckets

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an S3 bucket.

Amazon VPC interface endpoints

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an Amazon VPC interface endpoint.

Other records in the same hosted zone

If the AWS resource that you specify in **Endpoint** is a record or a group of records (for example, a group of weighted records) but is not another alias record, we recommend that you associate a health check with all of the records in the endpoint. For more information, see [What happens when you omit health checks? \(p. 544\)](#).

Record ID

Enter a value that uniquely identifies the primary and secondary records.

Values specific for geolocation records

When you create geolocation records, you specify the following values.

Topics

- [Routing policy \(p. 413\)](#)
- [Record name \(p. 413\)](#)
- [Record type \(p. 413\)](#)
- [TTL \(seconds\) \(p. 413\)](#)
- [Value/Route traffic to \(p. 414\)](#)
- [Location \(p. 414\)](#)
- [U.S. states \(p. 415\)](#)
- [Health check \(p. 415\)](#)
- [Record ID \(p. 416\)](#)

Routing policy

Choose **Geolocation**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Name** field.

Enter the same name for all of the records in the group of geolocation records.

For more information about record names, see [Record name \(p. 394\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the same value for all of the records in the group of geolocation records.

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

If you're associating this record with a health check, we recommend that you specify a TTL of 60 seconds or less so clients respond quickly to changes in health status.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. For all types except **CNAME**, you can enter more than one value. Enter each value on a separate line.

You can route traffic to, or specify the following values:

- **A — IPv4 address**
- **AAAA — IPv6 address**
- **CAA — Certificate Authority Authorization**
- **CNAME — Canonical name**
- **MX — Mail exchange**
- **NAPTR — Name Authority Pointer**
- **PTR — Pointer**
- **SPF — Sender Policy Framework**
- **SRV — Service locator**
- **TXT — Text**

For more information about the above values, see [Value/Route traffic to \(p. 394\)](#).

Location

When you configure Route 53 to respond to DNS queries based on the location that the queries originated from, select the continent or country for which you want Route 53 to respond with the settings in this record. If you want Route 53 to respond to DNS queries for individual states in the United States, select **United States** from the **Location** list, and then select the state under the **Sublocation** group.

Important

We recommend that you create one geolocation record that has a value of **Default for Location**. This covers geographic locations that you haven't created records for and IP addresses that Route 53 can't identify a location for.

You can't create non-geolocation records that have the same values for **Record name** and **Record type** as geolocation records.

For more information, see [Geolocation routing \(p. 372\)](#).

Here are the countries that Amazon Route 53 associates with each continent. The country codes are from ISO 3166. For more information, see the Wikipedia article [ISO 3166-1 alpha-2](#):

Africa (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

Antarctica (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

Europe (EU)

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

North America (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

Oceania (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

South America (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 doesn't support creating geolocation records for the following countries: Bouvet Island (BV), Christmas Island (CX), Western Sahara (EH), and Heard Island and McDonald Islands (HM).

No data is available about IP addresses for these countries.

U.S. states

When you configure Route 53 to respond to DNS queries based on the state of the United States that the queries originated from, select the state from the **U.S. states** list. United States territories (for example, Puerto Rico) are listed as countries in the **Location** list.

Important

Some IP addresses are associated with the United States, but not with an individual state. If you create records for all of the states in the United States, we recommend that you also create a record for the United States to route queries for these unassociated IP addresses. If you don't create a record for the United States, Route 53 responds to DNS queries from unassociated United States IP addresses with settings from the default geolocation record (if you created one) or with a "no answer" response.

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate Target Health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain Name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain Name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

For geolocation records, if an endpoint is unhealthy, Route 53 looks for a record for the larger, associated geographic Region. For example, suppose you have records for a state in the United States, for the United States, for North America, and for all locations (**Location** is **Default**). If the endpoint for the state record is unhealthy, Route 53 checks the records for the United States, for North America, and for all locations, in that order, until it finds a record that has a healthy endpoint. If all applicable records are unhealthy, including the record for all locations, Route 53 responds to the DNS query using the value for the record for the smallest geographic region.

Record ID

Enter a value that uniquely identifies this record in the group of geolocation records.

Values specific for geolocation alias records

When you create geolocation alias records, you specify the following values.

For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

Topics

- [Routing policy \(p. 417\)](#)
- [Record name \(p. 417\)](#)
- [Record type \(p. 417\)](#)
- [Value/Route traffic to \(p. 418\)](#)
- [Location \(p. 418\)](#)
- [U.S. states \(p. 419\)](#)
- [Health check \(p. 419\)](#)
- [Evaluate target health \(p. 420\)](#)
- [Record ID \(p. 421\)](#)

Routing policy

Choose **Geolocation**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for all of the records in the group of geolocation records.

For more information about record names, see [Record name \(p. 397\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the applicable value based on the AWS resource that you're routing traffic to. Select the same value for all of the records in the group of geolocation records:

API Gateway custom regional API or edge-optimized API

Select **A — IPv4 address**.

Amazon VPC interface endpoints

Select **A — IPv4 address**.

CloudFront distribution

Select **A — IPv4 address**.

If IPv6 is enabled for the distribution, create two records, one with a value of **A — IPv4 address** for **Record type**, and one with a value of **AAAA — IPv6 address**.

Elastic Beanstalk environment that has regionalized subdomains

Select **A — IPv4 address**.

ELB load balancer

Select A — IPv4 address or AAAA — IPv6 address

Amazon S3 bucket

Select A — IPv4 address

Another record in this hosted zone

Select the type of the record that you're creating the alias for. All types are supported except **NS** and **SOA**.

Note

If you're creating an alias record that has the same name as the hosted zone (known as the *zone apex*), you can't route traffic to a record for which the value of **Record type** is **CNAME**.

This is because the alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

Value/Route traffic to

The value that you choose from the list or that you type in the field depends on the AWS resource that you're routing traffic to.

For information about what AWS resources you can target, see [Value/route traffic to \(p. 397\)](#).

For more information about how to configure Route 53 to route traffic to specific AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Location

When you configure Route 53 to respond to DNS queries based on the location that the queries originated from, select the continent or country for which you want Route 53 to respond with the settings in this record. If you want Route 53 to respond to DNS queries for individual states in the United States, select **United States** from the **Location** list, and then select the state from the **U.S. states** list.

Important

We recommend that you create one geolocation record that has a value of **Default** for **Location**.

This covers geographic locations that you haven't created records for and IP addresses that Route 53 can't identify a location for.

You can't create non-geolocation records that have the same values for **Record name** and **Record type** as geolocation records.

For more information, see [Geolocation routing \(p. 372\)](#).

Here are the countries that Amazon Route 53 associates with each continent. The country codes are from ISO 3166. For more information, see the Wikipedia article [ISO 3166-1 alpha-2](#):

Africa (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

Antarctica (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

Europe (EU)

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

North America (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

Oceania (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

South America (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 doesn't support creating geolocation records for the following countries: Bouvet Island (BV), Christmas Island (CX), Western Sahara (EH), and Heard Island and McDonald Islands (HM).

No data is available about IP addresses for these countries.

U.S. states

When you configure Route 53 to respond to DNS queries based on the state of the United States that the queries originated from, select the state from the **U.S. states** list. United States territories (for example, Puerto Rico) are listed as countries in the **Location** list.

Important

Some IP addresses are associated with the United States, but not with an individual state. If you create records for all of the states in the United States, we recommend that you also create a record for the United States to route queries for these unassociated IP addresses. If you don't create a record for the United States, Route 53 responds to DNS queries from unassociated United States IP addresses with settings from the default geolocation record (if you created one) or with a "no answer" response.

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate target health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

For geolocation records, if an endpoint is unhealthy, Route 53 looks for a record for the larger, associated geographic Region. For example, suppose you have records for a state in the United States, for the United States, for North America, and for all locations (**Location** is **Default**). If the endpoint for the state record is unhealthy, Route 53 checks the records for the United States, for North America, and for all locations, in that order, until it finds a record that has a healthy endpoint. If all applicable records are unhealthy, including the record for all locations, Route 53 responds to the DNS query using the value for the record for the smallest geographic region.

Evaluate target health

Select **Yes** if you want Route 53 to determine whether to respond to DNS queries using this record by checking the health of the resource specified by **Endpoint**.

Note the following:

API Gateway custom regional APIs and edge-optimized APIs

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an API Gateway custom Regional API or an edge-optimized API.

CloudFront distributions

You can't set **Evaluate target health** to **Yes** when the endpoint is a CloudFront distribution.

Elastic Beanstalk environments that have regionalized subdomains

If you specify an Elastic Beanstalk environment in **Endpoint** and the environment contains an ELB load balancer, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. (An environment automatically contains an ELB load balancer if it includes more than one Amazon EC2 instance.) If you set **Evaluate target health** to **Yes** and either no Amazon EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other available resources that are healthy, if any.

If the environment contains a single Amazon EC2 instance, there are no special requirements.

ELB load balancers

Health checking behavior depends on the type of load balancer:

- **Classic Load Balancers** – If you specify an ELB Classic Load Balancer in **Endpoint**, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. If you set **Evaluate target health** to **Yes** and either no EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other resources.
- **Application and Network Load Balancers** – If you specify an ELB Application or Network Load Balancer and you set **Evaluate target health** to **Yes**, Route 53 routes queries to the load balancer based on the health of the target groups that are associated with the load balancer:
 - For an Application or Network Load Balancer to be considered healthy, every target group that contains targets must contain at least one healthy target. If any target group contains only unhealthy targets, the load balancer is considered unhealthy, and Route 53 routes queries to other resources.
 - A target group that has no registered targets is considered unhealthy.

Note

When you create a load balancer, you configure settings for Elastic Load Balancing health checks; they're not Route 53 health checks, but they perform a similar function. Do not create Route 53 health checks for the EC2 instances that you register with an ELB load balancer.

S3 buckets

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an S3 bucket.

Amazon VPC interface endpoints

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an Amazon VPC interface endpoint.

Other records in the same hosted zone

If the AWS resource that you specify in **Endpoint** is a record or a group of records (for example, a group of weighted records) but is not another alias record, we recommend that you associate a health check with all of the records in the endpoint. For more information, see [What happens when you omit health checks? \(p. 544\)](#).

Record ID

Enter a value that uniquely identifies this record in the group of geolocation records.

Values specific for latency records

When you create latency records, you specify the following values.

Topics

- [Routing policy \(p. 422\)](#)
- [Record name \(p. 422\)](#)
- [Record type \(p. 422\)](#)
- [TTL \(seconds\) \(p. 422\)](#)
- [Value/Route traffic to \(p. 423\)](#)
- [Region \(p. 423\)](#)
- [Health check \(p. 423\)](#)
- [Record ID \(p. 424\)](#)

Routing policy

Choose **Latency**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for all of the records in the group of latency records.

For more information about record names, see [Record name \(p. 394\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the value for **Type** based on how you want Route 53 to respond to DNS queries.

Select the same value for all of the records in the group of latency records.

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

If you're associating this record with a health check, we recommend that you specify a TTL of 60 seconds or less so clients respond quickly to changes in health status.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. For all types except **CNAME**, you can enter more than one value. Enter each value on a separate line.

You can route traffic to, or specify the following values:

- **A — IPv4 address**
- **AAAA — IPv6 address**
- **CAA — Certificate Authority Authorization**
- **CNAME — Canonical name**
- **MX — Mail exchange**
- **NAPTR — Name Authority Pointer**
- **PTR — Pointer**
- **SPF — Sender Policy Framework**
- **SRV — Service locator**
- **TXT — Text**

For more information about the above values, see [Value/Route traffic to \(p. 394\)](#).

Region

The Amazon EC2 Region where the resource that you specified in this record resides. Route 53 recommends an Amazon EC2 Region based on other values that you've specified. We recommend that you not change this value.

Note the following:

- You can only create one latency record for each Amazon EC2 Region.
- You aren't required to create latency records for all Amazon EC2 Regions. Route 53 chooses the Region with the best latency from among the Regions that you create latency records for.
- You can't create non-latency records that have the same values for **Record name** and **Record type** as latency records.
- If you create a record tagged with the Region **cn-north-1**, Route 53 always responds to queries from within China using this record, regardless of the latency.

For more information about using latency records, see [Latency-based routing \(p. 377\)](#).

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate target health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Record ID

Enter a value that uniquely identifies this record in the group of latency records.

Values specific for latency alias records

When you create latency alias records, you specify the following values.

For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

Topics

- [Routing policy \(p. 425\)](#)
- [Record name \(p. 425\)](#)
- [Record type \(p. 425\)](#)
- [Value/Route traffic to \(p. 426\)](#)
- [Region \(p. 426\)](#)
- [Health check \(p. 426\)](#)
- [Evaluate target health \(p. 427\)](#)
- [Record ID \(p. 428\)](#)

Routing policy

Choose **Latency**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for all of the records in the group of latency records.

For more information about record names, see [Record name \(p. 397\)](#)

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the applicable value based on the AWS resource that you're routing traffic to:

API Gateway custom regional API or edge-optimized API

Select **A — IPv4 address**.

Amazon VPC interface endpoints

Select **A — IPv4 address**.

CloudFront distribution

Select **A — IPv4 address**.

If IPv6 is enabled for the distribution, create two records, one with a value of **A — IPv4 address** for **Record type**, and one with a value of **AAAA — IPv6 address**.

Elastic Beanstalk environment that has regionalized subdomains

Select **A — IPv4 address**

ELB load balancer

Select A — IPv4 address or AAAA — IPv6 address

Amazon S3 bucket

Select A — IPv4 address

Another record in this hosted zone

Select the type of the record that you're creating the alias for. All types are supported except **NS** and **SOA**.

Note

If you're creating an alias record that has the same name as the hosted zone (known as the *zone apex*), you can't route traffic to a record for which the value of **Record type** is **CNAME**. This is because the alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

Select the same value for all of the records in the group of latency records.

Value/Route traffic to

The value that you choose from the list or that you type in the field depends on the AWS resource that you're routing traffic to.

For information about what AWS resources you can target, see [Value/route traffic to \(p. 397\)](#).

For more information about how to configure Route 53 to route traffic to specific AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Region

The Amazon EC2 region where the resource that you specified in this record resides. Route 53 recommends an Amazon EC2 Region based on other values that you've specified. We recommend that you not change this value.

Note the following:

- You can only create one latency record for each Amazon EC2 Region.
- You aren't required to create latency records for all Amazon EC2 Regions. Route 53 chooses the Region with the best latency from among the Regions that you create latency records for.
- You can't create non-latency records that have the same values for **Record name** and **Record type** as latency records.
- If you create a record tagged with the Region **cn-north-1**, Route 53 always responds to queries from within China using this record, regardless of the latency.

For more information about using latency records, see [Latency-based routing \(p. 377\)](#).

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate target health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain Name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Evaluate target health

Select **Yes** if you want Route 53 to determine whether to respond to DNS queries using this record by checking the health of the resource specified by **Endpoint**.

Note the following:

API Gateway custom regional APIs and edge-optimized APIs

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an API Gateway custom regional API or an edge-optimized API.

CloudFront distributions

You can't set **Evaluate Target Health** to **Yes** when the endpoint is a CloudFront distribution.

Elastic Beanstalk environments that have regionalized subdomains

If you specify an Elastic Beanstalk environment in **Endpoint** and the environment contains an ELB load balancer, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. (An environment automatically contains an ELB load balancer if it includes more than one Amazon EC2 instance.) If you set **Evaluate target health** to **Yes** and either no Amazon EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other available resources that are healthy, if any.

If the environment contains a single Amazon EC2 instance, there are no special requirements.

ELB load balancers

Health checking behavior depends on the type of load balancer:

- **Classic Load Balancers** – If you specify an ELB Classic Load Balancer in **Endpoint**, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. If you set **Evaluate target health** to **Yes** and either no EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other resources.
- **Application and Network Load Balancers** – If you specify an ELB Application or Network Load Balancer and you set **Evaluate target health** to **Yes**, Route 53 routes queries to the load balancer based on the health of the target groups that are associated with the load balancer:

- For an Application or Network Load Balancer to be considered healthy, every target group that contains targets must contain at least one healthy target. If any target group contains only unhealthy targets, the load balancer is considered unhealthy, and Route 53 routes queries to other resources.
- A target group that has no registered targets is considered unhealthy.

Note

When you create a load balancer, you configure settings for Elastic Load Balancing health checks; they're not Route 53 health checks, but they perform a similar function. Do not create Route 53 health checks for the EC2 instances that you register with an ELB load balancer.

S3 buckets

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an S3 bucket.

Amazon VPC interface endpoints

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an Amazon VPC interface endpoint.

Other records in the same hosted zone

If the AWS resource that you specify in **Endpoint** is a record or a group of records (for example, a group of weighted records) but is not another alias record, we recommend that you associate a health check with all of the records in the endpoint. For more information, see [What happens when you omit health checks? \(p. 544\)](#).

Record ID

Enter a value that uniquely identifies this record in the group of latency records.

Values specific for multivalue answer records

When you create multivalue answer records, you specify the following values.

Note

Creating multivalue answer alias records is not supported.

Topics

- [Routing policy \(p. 429\)](#)
- [Record name \(p. 429\)](#)
- [Record type \(p. 429\)](#)
- [TTL \(seconds\) \(p. 429\)](#)
- [Value/Route traffic to \(p. 430\)](#)
- [Health check \(p. 430\)](#)
- [Record ID \(p. 431\)](#)

Routing policy

Choose **Multivalue answer**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for all of the records in the group of weighted records.

For more information about record names, see [Record name \(p. 394\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select any value except **NS** or **CNAME**.

Select the same value for all of the records in the group of multivalue answer records.

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

If you're associating this record with a health check, we recommend that you specify a TTL of 60 seconds or less so clients respond quickly to changes in health status.

Note

If you create two or more multivalue answer records that have the same name and type, you are using the console, and you specify different values for **TTL**, Route 53 changes the value of **TTL** for all of the records to the last value that you specified.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. If you enter more than one value, enter each value on a separate line.

You can route traffic to, or specify the following values:

- **A — IPv4 address**
- **AAAA — IPv6 address**
- **CAA — Certificate Authority Authorization**
- **CNAME — Canonical name**
- **MX — Mail exchange**
- **NAPTR — Name Authority Pointer**
- **PTR — Pointer**
- **SPF — Sender Policy Framework**
- **SRV — Service locator**
- **TXT — Text**

For more information about the above values, see [Value/Route traffic to \(p. 394\)](#).

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate target health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Record ID

Enter a value that uniquely identifies this record in the group of multivalue answer records.

Values specific for weighted records

When you create weighted records, you specify the following values.

Topics

- [Routing policy \(p. 432\)](#)
- [Record name \(p. 432\)](#)
- [Record type \(p. 432\)](#)
- [TTL \(seconds\) \(p. 432\)](#)
- [Value/Route traffic to \(p. 433\)](#)
- [Weight \(p. 433\)](#)
- [Health check \(p. 433\)](#)
- [Record ID \(p. 434\)](#)

Routing policy

Select **Weighted**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Record name** field.

Enter the same name for all of the records in the group of weighted records.

For more information about record names, see [Record name \(p. 394\)](#).

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the same value for all of the records in the group of weighted records.

TTL (seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you reduce the number of calls that DNS recursive resolvers must make to Route 53 to get the latest information in this record. This has the effect of reducing latency and reducing your bill for Route 53 service. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

However, if you specify a longer value for TTL, it takes longer for changes to the record (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods before they ask Route 53 for the latest information. If you're changing settings for a domain or subdomain that's already in use, we recommend that you initially specify a shorter value, such as 300 seconds, and increase the value after you confirm that the new settings are correct.

If you're associating this record with a health check, we recommend that you specify a TTL of 60 seconds or less so clients respond quickly to changes in health status.

You must specify the same value for **TTL** for all of the records in this group of weighted records.

Note

If you create two or more weighted records that have the same name and type, and you specify different values for **TTL**, Route 53 changes the value of **TTL** for all of the records to the last value that you specified.

If a group of weighted records includes one or more weighted alias records that are routing traffic to an ELB load balancer, we recommend that you specify a TTL of 60 seconds for all of the non-alias weighted records that have the same name and type. Values other than 60 seconds (the TTL for load balancers) will change the effect of the values that you specify for **Weight**.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter a value that is appropriate for the value of **Record type**. For all types except **CNAME**, you can enter more than one value. Enter each value on a separate line.

You can route traffic to, or specify the following values:

- **A — IPv4 address**
- **AAAA — IPv6 address**
- **CAA — Certificate Authority Authorization**
- **CNAME — Canonical name**
- **MX — Mail exchange**
- **NAPTR — Name Authority Pointer**
- **PTR — Pointer**
- **SPF — Sender Policy Framework**
- **SRV — Service locator**
- **TXT — Text**

For more information about the above values, see [Value/Route traffic to \(p. 394\)](#).

Weight

A value that determines the proportion of DNS queries that Route 53 responds to using the current record. Route 53 calculates the sum of the weights for the records that have the same combination of DNS name and type. Route 53 then responds to queries based on the ratio of a resource's weight to the total.

You can't create non-weighted records that have the same values for **Record name** and **Record type** as weighted records.

Enter an integer between 0 and 255. To disable routing to a resource, set **Weight** to 0. If you set **Weight** to 0 for all of the records in the group, traffic is routed to all resources with equal probability. This ensures that you don't accidentally disable routing for a group of weighted records.

The effect of setting **Weight** to 0 is different when you associate health checks with weighted records. For more information, see [How Amazon Route 53 chooses records when health checking is configured \(p. 546\)](#).

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53

checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate target health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Record ID

Enter a value that uniquely identifies this record in the group of weighted records.

Values specific for weighted alias records

When you create weighted alias records, you specify the following values. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

Topics

- [Routing policy \(p. 435\)](#)
- [Record name \(p. 435\)](#)
- [Record type \(p. 435\)](#)
- [Value/Route traffic to \(p. 436\)](#)
- [Weight \(p. 436\)](#)
- [Health check \(p. 436\)](#)
- [Evaluate target health \(p. 437\)](#)
- [Record ID \(p. 438\)](#)

Routing policy

Choose **Weighted**.

Record name

Enter the name of the domain or subdomain that you want to route traffic for. The default value is the name of the hosted zone.

Note

If you're creating a record that has the same name as the hosted zone, don't enter a value (for example, an @ symbol) in the **Name** field.

Enter the same name for all of the records in the group of weighted records.

For more information about record names, see [Record name \(p. 397\)](#)

Record type

The DNS record type. For more information, see [Supported DNS record types \(p. 382\)](#).

Select the applicable value based on the AWS resource that you're routing traffic to:

API Gateway custom regional API or edge-optimized API

Select **A — IPv4 address**.

Amazon VPC interface endpoints

Select **A — IPv4 address**.

CloudFront distribution

Select **A — IPv4 address**.

If IPv6 is enabled for the distribution, create two records, one with a value of **A — IPv4 address** for **Record type**, and one with a value of **AAAA — IPv6 address**.

Elastic Beanstalk environment that has regionalized subdomains

Select **A — IPv4 address**

ELB load balancer

Select **A — IPv4 address or AAAA — IPv6 address**

Amazon S3 bucket

Select A — IPv4 address

Another record in this hosted zone

Select the type of the record that you're creating the alias for. All types are supported except **NS** and **SOA**.

Note

If you're creating an alias record that has the same name as the hosted zone (known as the *zone apex*), you can't route traffic to a record for which the value of **Record type** is **CNAME**. This is because the alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

Select the same value for all of the records in the group of weighted records.

Value/Route traffic to

The value that you choose from the list or that you type in the field depends on the AWS resource that you're routing traffic to.

For information about what AWS resources you can target, see [Value/route traffic to \(p. 397\)](#).

For more information about how to configure Route 53 to route traffic to specific AWS resources, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Weight

A value that determines the proportion of DNS queries that Route 53 responds to using the current record. Route 53 calculates the sum of the weights for the records that have the same combination of DNS name and type. Route 53 then responds to queries based on the ratio of a resource's weight to the total.

You can't create non-weighted records that have the same values for **Record name** and **Record type** as weighted records.

Enter an integer between 0 and 255. To disable routing to a resource, set **Weight** to 0. If you set **Weight** to 0 for all of the records in the group, traffic is routed to all resources with equal probability. This ensures that you don't accidentally disable routing for a group of weighted records.

The effect of setting **Weight** to 0 is different when you associate health checks with weighted records. For more information, see [How Amazon Route 53 chooses records when health checking is configured \(p. 546\)](#).

Health check

Select a health check if you want Route 53 to check the health of a specified endpoint and to respond to DNS queries using this record only when the endpoint is healthy.

Route 53 doesn't check the health of the endpoint specified in the record, for example, the endpoint specified by the IP address in the **Value** field. When you select a health check for a record, Route 53 checks the health of the endpoint that you specified in the health check. For information about how Route 53 determines whether an endpoint is healthy, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Associating a health check with a record is useful only when Route 53 is choosing between two or more records to respond to a DNS query, and you want Route 53 to base the choice in part on the status of a health check. Use health checks only in the following configurations:

- You're checking the health of all of the records in a group of records that have the same name, type, and routing policy (such as failover or weighted records), and you specify health check IDs for all the records. If the health check for a record specifies an endpoint that is not healthy, Route 53 stops responding to queries using the value for that record.
- You select **Yes** for **Evaluate target health** for an alias record or the records in a group of failover alias, geolocation alias, latency alias, or weighted alias record. If the alias records reference non-alias records in the same hosted zone, you must also specify health checks for the referenced records.

If your health checks specify the endpoint only by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (example.com).

Important

In this configuration, if you create a health check for which the value of **Domain name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

Evaluate target health

Select **Yes** if you want Route 53 to determine whether to respond to DNS queries using this record by checking the health of the resource specified by **Endpoint**.

Note the following:

API Gateway custom regional APIs and edge-optimized APIs

There are no special requirements for setting **Evaluate target health** to **Yes** when the endpoint is an API Gateway custom Regional API or an edge-optimized API.

CloudFront distributions

You can't set **Evaluate target health** to **Yes** when the endpoint is a CloudFront distribution.

Elastic Beanstalk environments that have regionalized subdomains

If you specify an Elastic Beanstalk environment in **Endpoint** and the environment contains an ELB load balancer, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. (An environment automatically contains an ELB load balancer if it includes more than one Amazon EC2 instance.) If you set **Evaluate target health** to **Yes** and either no Amazon EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other available resources that are healthy, if any.

If the environment contains a single Amazon EC2 instance, there are no special requirements.

ELB load balancers

Health checking behavior depends on the type of load balancer:

- **Classic Load Balancers** – If you specify an ELB Classic Load Balancer in **Endpoint**, Elastic Load Balancing routes queries only to the healthy Amazon EC2 instances that are registered with the load balancer. If you set **Evaluate Target Health** to **Yes** and either no EC2 instances are healthy or the load balancer itself is unhealthy, Route 53 routes queries to other resources.
- **Application and Network Load Balancers** – If you specify an ELB Application or Network Load Balancer and you set **Evaluate Target Health** to **Yes**, Route 53 routes queries to the load balancer based on the health of the target groups that are associated with the load balancer:
 - For an Application or Network Load Balancer to be considered healthy, every target group that contains targets must contain at least one healthy target. If any target group contains only unhealthy targets, the load balancer is considered unhealthy, and Route 53 routes queries to other resources.

- A target group that has no registered targets is considered unhealthy.

Note

When you create a load balancer, you configure settings for Elastic Load Balancing health checks; they're not Route 53 health checks, but they perform a similar function. Do not create Route 53 health checks for the EC2 instances that you register with an ELB load balancer.

S3 buckets

There are no special requirements for setting **Evaluate target health to Yes** when the endpoint is an S3 bucket.

Amazon VPC interface endpoints

There are no special requirements for setting **Evaluate target health to Yes** when the endpoint is an Amazon VPC interface endpoint.

Other records in the same hosted zone

If the AWS resource that you specify in **Endpoint** is a record or a group of records (for example, a group of weighted records) but is not another alias record, we recommend that you associate a health check with all of the records in the endpoint. For more information, see [What happens when you omit health checks? \(p. 544\)](#).

Record ID

Enter a value that uniquely identifies this record in the group of weighted records.

Creating records by importing a zone file

If you're migrating from another DNS service provider, and if your current DNS service provider lets you export your current DNS settings to a zone file, you can quickly create all of the records for an Amazon Route 53 hosted zone by importing a zone file.

Note

A zone file uses a standard format known as BIND to represent records in a text format. For information about the format of a zone file, see the Wikipedia entry [Zone file](#). Additional information is available in [RFC 1034, Domain Names—Concepts and Facilities](#) section 3.6.1, and [RFC 1035, Domain Names—Implementation and Specification](#) section 5.

If you want to create records by importing a zone file, note the following:

- The zone file must be in RFC-compliant format.
- The domain name of the records in the zone file must match the name of the hosted zone.
- Route 53 supports the \$ORIGIN and \$TTL keywords. If the zone file includes \$GENERATE or \$INCLUDE keywords, the import fails and Route 53 returns an error.
- When you import the zone file, Route 53 ignores the SOA record in the zone file. Route 53 also ignores any NS records that have the same name as the hosted zone.
- You can import a maximum of 1000 records. If you need to import more than 1000 records, you might be able to use the [BIND to Amazon Route 53 Conversion Tool](#).
- If the hosted zone already contains records that appear in the zone file, the import process fails, and no records are created.
- We recommend that you review the contents of the zone file to confirm that record names include or exclude a trailing dot as appropriate:
 - When the name of a record in the zone file includes a trailing dot (example.com.), the import process interprets the name as a fully qualified domain name and creates a Route 53 record with that name.

- When the name of a record in the zone file does not include a trailing dot (www), the import process concatenates that name with the domain name in the zone file (example.com) and creates a Route 53 record with the concatenated name (www.example.com).

If the export process doesn't add a trailing dot to the fully qualified domain names of a record, the Route 53 import process adds the domain name to the name of the record. For example, suppose you're importing records into the hosted zone example.com and the name of an MX record in the zone file is mail.example.com, with no trailing dot. The Route 53 import process creates an MX record named mail.example.com.example.com.

Important

For CNAME, MX, PTR, and SRV records, this behavior also applies to the domain name that is included in the RDATA value. For example, suppose you have a zone file for example.com. If a CNAME record in the zone file (support, without a trailing dot) has an RDATA value of www.example.com (also without a trailing dot), the import process creates a Route 53 record with the name support.example.com that routes traffic to www.example.com.example.com. Before you import your zone file, review RDATA values and update as applicable.

Route 53 doesn't support exporting records to a zone file.

To create records by importing a zone file

1. Get a zone file from the DNS service provider that is currently servicing the domain. The process and terminology vary from one service provider to another. Refer to your provider's interface and documentation for information about exporting or saving your records in a zone file or a BIND file.

If the process isn't obvious, try asking your current DNS provider's customer support for your *records list* or *zone file* information.
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Hosted zones**.
4. On the **Hosted zones** page, create a new hosted zone:
 - a. Choose **Create hosted zone**.
 - b. Enter the name of your domain and, optionally, a comment.
 - c. Choose **Create**.
5. Choose **Import zone file**.
6. In the **Import zone file** pane, paste the contents of your zone file into the **Zone file** text box.
7. Choose **Import**.

Note

Depending on the number of records in your zone file, you might have to wait a few minutes for the records to be created.

8. If you're using another DNS service for the domain (which is common if you registered the domain with another registrar), migrate DNS service to Route 53. When that step is complete, your registrar will start to identify Route 53 as your DNS service in response to DNS queries for your domain, and the queries will start being sent to Route 53 DNS servers. (Typically, there's a day or two of delay before DNS queries start being routed to Route 53 because information about your previous DNS service is cached on DNS resolvers for that long.) For more information, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Editing records

The following procedure explains how to edit records using the Amazon Route 53 console. For information about how to edit records using the Route 53 API, see [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

Note

Your changes to records take time to propagate to the Route 53 DNS servers. Currently, the only way to verify that changes have propagated is to use the [GetChange](#) API action. Changes generally propagate to all Route 53 name servers within 60 seconds.

To edit records using the Route 53 console

1. If you're not editing alias records, skip to step 2.

If you're editing alias records that route traffic to ELB Classic, Application, or Network Load Balancers, and if you created your Route 53 hosted zone and your load balancer using different accounts, perform the procedure [Getting the DNS name for an ELB load balancer \(p. 393\)](#) to get the DNS name for the load balancer.

If you're editing alias records for any other AWS resource, skip to step 2.

2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Hosted zones**.
4. On the **Hosted Zones** page, choose the row for the hosted zone that contains the records that you want to edit.
5. Select the row for the record that you want to edit, and then enter your changes in the **Edit record** pane.
6. Enter the applicable values. For more information, see [Values that you specify when you create or edit Amazon Route 53 records \(p. 393\)](#).
7. Choose **Save changes**.
8. If you're editing multiple records, repeat steps 5 through 7.

Deleting records

The following procedure explains how to delete records using the Route 53 console. For information about how to delete records using the Route 53 API, see [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

Note

Your changes to records take time to propagate to the Route 53 DNS servers. Currently, the only way to verify that changes have propagated is to use the [GetChange](#) API action. Changes generally propagate to all Route 53 name servers within 60 seconds.

To delete records

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. On the Hosted Zones page, choose the row for the hosted zone that contains records that you want to delete.
3. In the list of records, select the record that you want to delete.

To select multiple, consecutive records, choose the first row, hold the **Shift** key, and choose the last row. To select multiple, nonconsecutive records, choose the first row, hold the **Ctrl** key, and choose additional rows.

You can't delete the records that have a value of **NS** or **SOA** for **Type**.

4. Choose **Delete**.
5. Choose **Delete** to close the dialog box.

Listing records

The following procedure explains how to use the Amazon Route 53 console to list the records in a hosted zone. For information about how to list records using the Route 53 API, see [ListResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

To list records

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. On the **Hosted Zones** page, choose the name of a hosted zone.

To display only selected records, enter the applicable search criteria above the list of records. Search behavior depends on whether the hosted zone contains up to 2,000 records or more than 2,000 records:

Up to 2,000 records

- To display the records that have specific values, enter a value in the search bar and press **Enter**. For example, to display the records that have an IP address beginning with **192.0**, enter that value in the **Search** field and press **Enter**.
- To display only the records that have the same DNS record type, select **Record type** in the dropdown list, and enter the record type.
- To display only alias records, select **Aliase** in the dropdown list, and enter **Yes**.
- To display only weighted records, select **Routing policy** in the dropdown list, and enter **WEIGHTED**.

More than 2,000 records

- You can search only on record names, not on record values. You also can't filter based on the record type, or on alias or weighted records.
- For records that have three labels (three parts separated by dots), when you enter a value in the search field and press **Enter**, the Route 53 console automatically performs a wildcard search on the third label from the right in the record name. For example, suppose the hosted zone `example.com` contains 100 records named `record1.example.com` through `record100.example.com`. (`Record1` is the third label from the right.) Here's what happens when you search on the following values:
 - **record1** – The Route 53 console searches for `record1*.example.com`, which returns `record1.example.com`, `record10.example.com` through `record19.example.com`, and `record100.example.com`.
 - **record1.example.com** – As in the preceding example, the console searches for `record1*.example.com` and returns the same records.
 - **1** – The console searches for `1*.example.com` and returns no records.
 - **example** – The console searches for `example*.example.com` and returns no records.
 - **example.com** – In this example, the console doesn't perform a wildcard search. It returns all the records in the hosted zone.

Note

If the third label from the right contains one or more hyphens (such as `third-label.example.com`), and if you search for the part of the third label immediately

before the hyphen (third in this example), Route 53 won't return any records. Instead, either include the hyphen (search for third-) or omit the character immediately before the hyphen (search for thir).

- For records that have four or more labels, you must specify the exact name of the record. No wildcard searches are supported. For example, if the hosted zone includes a record named label4.record1.example.com, you can find that record only if you specify **label4.record1.example.com** in the search field.

Using traffic flow to route DNS traffic

Managing related records in a hosted zone can be challenging in the following circumstances:

- You have a lot of resources that perform the same operation, such as web servers that serve traffic for the same domain.
- You want to create a complex tree of records using [alias records](#) and a combination of [Route 53 routing policies](#), such as latency, failover, and weighted.

You can create records one at a time, but it's hard to keep track of the relationships among the records when you're reviewing the settings in the Route 53 console. Traffic flow greatly simplifies the process of creating and maintaining records in large and complex configurations.

Visual editor

The traffic flow visual editor lets you create complex trees of records and see the relationships among the records. For example, you might create a configuration in which latency alias records reference weighted records, and the weighted records reference your resources in multiple AWS Regions. Each configuration is known as a *traffic policy*. You can create as many traffic policies as you want at no charge.

Versioning

You can create multiple versions of a traffic policy so you don't have to start all over when your configuration changes. Old versions continue to exist until you delete them; there's a default limit of 1000 versions per traffic policy. You can optionally give each version a description.

Automatic record creation and updating

A traffic policy can represent dozens or even hundreds of records. Traffic flow lets you create all those records automatically by creating a *traffic policy record*. You specify the hosted zone and the name of the record at the root of the tree, such as example.com or www.example.com, and Route 53 automatically creates all the other records in the tree. The root record—the traffic policy record—appears in the list of records for your hosted zone; all the other records are hidden.

When you create a new version of a traffic policy, you can selectively update traffic policy records that you created using the previous traffic policy version. When you update a traffic policy record, Route 53 automatically updates all the other records in the tree. You can also quickly roll back changes by updating a traffic policy record again to use a previous version of a traffic policy.

Note

You can use traffic flow to create records only in public hosted zones.

Reuse for multiple records in different hosted zones

You can use a traffic policy to automatically create records in multiple public hosted zones. For example, if you're using the same web servers for multiple domain names, you can use the same traffic policy to create traffic policy records in the hosted zones for example.com, example.org, and example.net.

How Route 53 responds to DNS queries

When a client submits a query for the name of the root record, such as example.com or www.example.com, Route 53 responds to the query based on the configuration in the traffic policy that you used to create the corresponding traffic policy record.

Geoproximity routing policy

The geoproximity routing policy is available only if you use traffic flow. With geoproximity routing, you can route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another. For more information, see [Geoproximity routing \(traffic flow only\) \(p. 373\)](#).

Charge for traffic flow

There's a monthly charge for each traffic policy record. For more information, see the "Traffic Flow" section of [Amazon Route 53 pricing](#).

To minimize these charges, you can create one or more alias records in a hosted zone that reference a traffic policy record in that hosted zone. For example, you can create a traffic policy record for example.com and then create an alias record for www.example.com that references the traffic policy record.

Topics

- [Creating and managing traffic policies \(p. 443\)](#)
- [Creating and managing policy records \(p. 453\)](#)

Creating and managing traffic policies

Topics

- [Creating a traffic policy \(p. 443\)](#)
- [Values that you specify when you create a traffic policy \(p. 444\)](#)
- [Viewing a map that shows the effect of geoproximity settings \(p. 448\)](#)
- [Creating additional versions of a traffic policy \(p. 449\)](#)
- [Creating a traffic policy by importing a JSON document \(p. 450\)](#)
- [Viewing traffic policy versions and the associated policy records \(p. 451\)](#)
- [Deleting traffic policy versions and traffic policies \(p. 452\)](#)

Creating a traffic policy

To create a traffic policy, perform the following procedure.

To create a traffic policy

1. Design your configuration. For information about how complex DNS routing configurations work, see [Configuring DNS failover \(p. 536\)](#) in [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).
2. Based on the design for your configuration, create the health checks that you want to use for your endpoints.
3. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
4. In the navigation pane, choose **Traffic policies**.

5. Choose **Create traffic policy**.
6. On the **Name policy** page, specify the applicable values. For more information, see [Values that you specify when you create a traffic policy \(p. 444\)](#).
7. Choose **Next**.
8. On the **Create traffic policy policy name v1** page, specify the applicable values. For more information, see [Values that you specify when you create a traffic policy \(p. 444\)](#).

You can delete rules, endpoints, and branches of a traffic policy in the following ways:

- To delete a rule or an endpoint, click the x in the upper-right corner of the box.

Important

If you delete a rule that has child rules and endpoints, Amazon Route 53 also deletes all of the children.

- If you connect two rules to the same child rule or endpoint and you want to delete one of the connections, pause your cursor on the connection that you want to delete, and click the x for that connection.

9. Choose **Create traffic policy**.

10. *Optional:* On the **Create policy records with traffic policy** page, use the new traffic policy to create one or more policy records in one hosted zone. For more information, see [Values that you specify when you create or update a policy record \(p. 454\)](#). You can also create policy records later, either in the same hosted zone or in additional hosted zones.

If you don't want to create policy records now, choose **Skip this step**, and the console displays the list of traffic policies and policy records that you have created by using the current AWS account.

11. If you specified settings for policy records in the preceding step, choose **Create policy record**.

Values that you specify when you create a traffic policy

When you create a traffic policy, you specify the following values.

- the section called "Policy name"
- the section called "Version"
- the section called "Version description"
- the section called "DNS type"
- the section called "Connect to"
- the section called "Value type"
- the section called "Value"

Policy name

Enter a name that describes the traffic policy. This value appears in the list of traffic policies in the console. You can't change the name of a traffic policy after you create it.

Version

This value is assigned automatically by Amazon Route 53 when you create a traffic policy or a new version of an existing policy.

Version description

Enter a description that applies to this version of the traffic policy. This value appears in the list of traffic policy versions in the console.

DNS type

Choose the DNS type that you want Amazon Route 53 to assign to all of the records when you create a policy record by using this traffic policy version. For a list of supported types, see [Supported DNS record types \(p. 382\)](#).

Important

If you're creating a new version of an existing traffic policy, you can change the DNS type. However, you can't edit a policy record and choose a traffic policy version that has a DNS type that is different from the traffic policy version that you used to create the policy record. For example, if you created a policy record by using a traffic policy version that has a **DNS type** of A, you can't edit the policy record and choose a traffic policy version that has any other value for **DNS type**.

If you want to route traffic to the following AWS resources, choose the applicable value:

- **CloudFront distribution** – Choose **A: IP address in IPv4 format**.
- **ELB load balancer** – Choose either **A: IP address in IPv4 format** or **AAAA: IP address in IPv6 format**.
- **Amazon S3 bucket configured as a website endpoint**: Choose **A: IP address in IPv4 format**.

Connect to

Choose the applicable rule or endpoint based on the design for your configuration.

Failover rule

Choose this option when you want to configure active-passive failover, in which one resource takes all traffic when it's available and the other resource takes all traffic when the first resource isn't available.

For more information, see [Active-passive failover \(p. 548\)](#).

Geolocation rule

Choose this option when you want Amazon Route 53 to respond to DNS queries based on the location of your users.

For more information, see [Geolocation routing \(p. 372\)](#).

When you choose **Geolocation rule**, you also choose the country or the state in the United States that requests originate from.

Latency rule

Choose this option when you have resources in multiple Amazon EC2 data centers that perform the same function, and you want Route 53 to respond to DNS queries with the resources that provide the best latency.

When you choose **Latency rule**, you also choose an AWS Region.

For more information, see [Latency-based routing \(p. 377\)](#).

Geoproximity rule

Choose this option when you want Route 53 to respond to DNS queries based on the location of your resources and optionally on a bias that you specify. The bias allows you to send more traffic to a resource or more traffic away from a resource.

When you choose **Geoproximity rule**, enter the following values:

Endpoint location

Choose the applicable value:

- **Custom (enter coordinates)** – If your endpoint is not an AWS resource, choose **Custom (enter coordinates)**.
- **An AWS Region** – If your endpoint is an AWS resource, choose the AWS Region that you created the resource in.

Coordinates

If you chose **Custom (enter coordinates)** for **Endpoint location**, enter the latitude and longitude of the location of the resource. Note the following:

- Latitude represents the location south (negative) or north (positive) of the equator. Valid values are -90 degrees to 90 degrees.
- Longitude represents the location west (negative) or east (positive) of the prime meridian. Valid values are -180 degrees to 180 degrees.
- You can get latitude and longitude from some online mapping applications. For example, in Google Maps, the URL for a location specifies the latitude and longitude:

`https://www.google.com/maps/@47.608611,-122.3409953,20z`

- You can enter up to two decimals of precision, for example, **47.63**. If you specify a value with greater precision, Route 53 truncates the value to two places after the decimal. For latitude and for longitude at the equator, 0.01 degree is approximately 0.69 miles.

Bias

To optionally change the size of the geographic region from which Route 53 routes traffic to a resource, specify the applicable value for **Bias**:

- To expand the size of the geographic region from which Route 53 routes traffic to a resource, specify a positive integer from 1 to 99 for the bias. Route 53 shrinks the size of adjacent regions.
- To shrink the size of the geographic region from which Route 53 routes traffic to a resource, specify a negative bias of -1 to -99. Route 53 expands the size of adjacent regions.

Important

The effect of changing the value of **Bias** is relative, based on the location of other resources, rather than absolute, based on distance. As a result, the effect of a change is difficult to predict. For example, depending on where your resources are, changing the bias from 10 to 15 can mean the difference between adding or subtracting a significant amount of traffic from the New York City metropolitan area. We recommend that you change the bias in small increments and evaluate the results, and then make additional changes if appropriate.

For more information, see [Geoproximity routing \(traffic flow only\) \(p. 373\)](#).

Multivalue answer rule

Choose this option when you want Route 53 to respond to DNS queries with up to eight healthy answers selected approximately at random.

For more information, see [Multivalue answer routing \(p. 378\)](#).

Weighted rule

Choose this option when you have multiple resources that perform the same function (for example, web servers that serve the same website) and you want Route 53 to route traffic to those resources in proportions that you specify (for example, 1/3rd to one server and 2/3rds to the other).

When you choose **Weighted rule**, enter the weight that you want to apply to this rule.

For more information, see [Weighted routing \(p. 378\)](#).

Endpoint

Choose this option to specify the resource, such as a CloudFront distribution or an ELB load balancer, that you want to route DNS queries to.

Existing rule

Choose this option when you want to route DNS queries to an existing rule in this traffic policy. For example, you might create two or more geolocation rules that route queries for different countries to the same failover rule. The failover rule might then routes queries to two ELB load balancers.

This option isn't available if the traffic policy doesn't include any rules.

Existing endpoint

Choose this option when you want to route DNS queries to an existing endpoint. For example, if you have two failover rules, you might want to route DNS queries for both **On failover** (secondary) options to the same ELB load balancer.

This option isn't available if the traffic policy doesn't include any endpoints.

Value type

Choose the applicable option:

CloudFront distribution

Choose this option if you want to route traffic to a CloudFront distribution. The option is available only if you chose **A: IP address in IPv4 format** for **DNS type**.

ELB load balancer

Choose this option if you want to route traffic to an ELB load balancer. The option is available only if you chose either **A: IP address in IPv4 format** or **AAAA: IP address in IPv6 format** for **DNS type**.

S3 website endpoint

Choose this option if you want to route traffic to an Amazon S3 bucket that is configured as a website endpoint. The option is available only if you chose **A: IP address in IPv4 format** for **DNS type**.

Type **DNS type** value

Choose this option if you want Route 53 to respond to DNS queries using the value in the **Value** field. For example, if you chose **A** for the value of **DNS type** when you created this traffic policy, this option in the **Value type** list will be **Type A value**. This requires that you enter an IP address in IPv4 format in the **Value** field. Route 53 will respond to DNS queries that are routed to this endpoint with the IP address in the **Value** field.

Value

Choose or enter a value based on the option that you chose for **Value type**:

CloudFront distribution

Choose a CloudFront distribution from the list of distributions that are associated with the current AWS account.

ELB load balancer

Choose an ELB load balancer from the list of ELB load balancers that are associated with the current AWS account.

S3 website endpoint

Choose an Amazon S3 bucket from the list of Amazon S3 buckets that are configured as website endpoints and that are associated with the current AWS account.

Important

When you create a policy record based on this traffic policy, the bucket that you choose here must match the domain name (such as www.example.com) that you specify for **Policy record DNS name** in the policy record. If **Value** and **Policy record DNS name** don't match, Amazon S3 won't respond to DNS queries for the domain name.

Type DNS type value

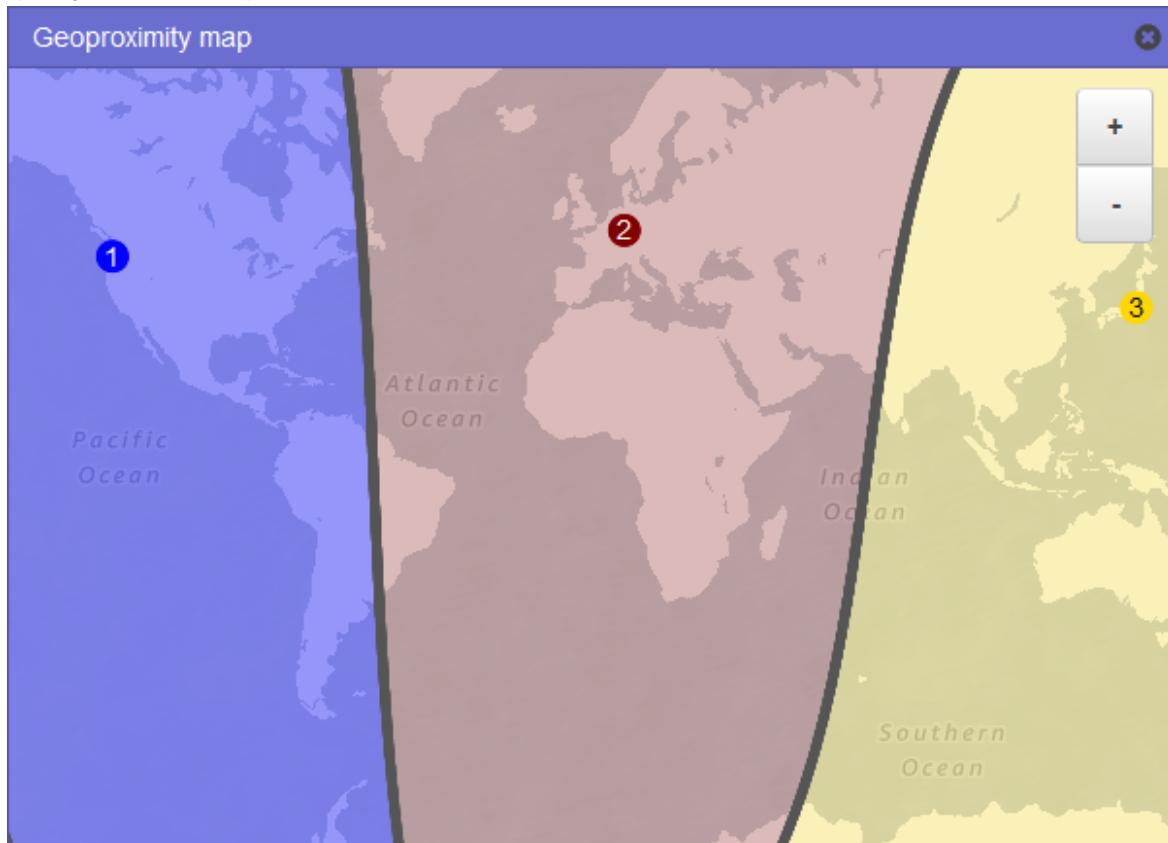
Enter a value that corresponds with the value that you specified for **DNS type** when you started this traffic policy. For example, if you chose **MX** for **DNS type**, enter two values: the priority that you want to assign to a mail server and the domain name of the mail server, such as 10 sydney.mail.example.com.

For more information about supported DNS types, see [Supported DNS record types \(p. 382\)](#).

Viewing a map that shows the effect of geoproximity settings

A *geoproximity rule* lets you specify the locations of your resources, both in AWS Regions and, using latitude and longitude, in non-AWS locations. When you create a geoproximity rule, Route 53 routes internet traffic to the resource that is closest to your users by default. You can also choose to route more or less traffic to a resource by specifying a bias that expands or shrinks the geographic area from which traffic is routed to a resource. For more information about geoproximity routing, see [Geoproximity routing \(traffic flow only\) \(p. 373\)](#).

You can display a map that shows the effect of your current geoproximity settings. For example, if you have resources in the US West (Oregon), EU (Frankfurt), and Asia Pacific (Tokyo) Regions, and if you don't specify a bias, the map looks like this.



To display the map for a geoproximity rule, choose the graph icon next to **Show geoproximity map**. (This icon appears at the top of the rule.) To hide the map, choose the icon again or choose the **x** in the upper right corner of the map.

Note the following:

- The map is accurate to within approximately 10 miles (16 kilometers).
- The map automatically adjusts when you add, edit, or delete regions, or when you change the bias setting for a region.
- The region number and color in each rule definition correspond with numbers and colors on the map.
- You can zoom in and zoom out to see more or less detail. Use the + and - buttons on the map, a touchpad, or the wheel on a mouse to change the zoom level.
- You can move the map around inside the map window to see specific areas. Use a touchpad, or click and drag the map with a mouse. You can also move the map window in the browser window.
- If you have more than one geoproximity rule in a policy, you can view the map for only one rule at a time.

Creating additional versions of a traffic policy

When you edit a traffic policy, Amazon Route 53 automatically creates another version of the traffic policy and retains the previous versions unless you choose to delete them. The new version has the same name as the traffic policy that you're editing; it's distinguished from the original version by a version number that Route 53 increments automatically. You can base the new version of a traffic policy on any existing version of a traffic policy that has the same name.

Route 53 doesn't reuse version numbers for new versions of a given traffic policy. For example, if you create three versions of **MyTrafficPolicy**, delete the last two versions, and then create another version, the new version is version 4. By retaining the previous versions, Route 53 ensures that you can roll back to a previous configuration if a new configuration doesn't route traffic as you wanted it to.

To create a new traffic policy version, perform the following procedure.

To create another version of a traffic policy

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Traffic policies**.
3. Choose the name of the traffic policy that you want to create a new version of.
4. In the **Traffic policy versions** table at the top of the page, select the check box for the traffic policy version that you want to use as a basis for the new traffic policy version.
5. Choose **Edit policy as new version**.
6. On the **Update description** page, enter a description for the new traffic policy version. We recommend that you specify a description that distinguishes this version from other versions of the same traffic policy. When you create a new policy record, the value that you specify appears in the list of available versions for this traffic policy.
7. Choose **Next**.
8. Update the configuration as applicable. For more information, see [Values that you specify when you create a traffic policy \(p. 444\)](#).

You can delete rules, endpoints, and branches of a traffic policy in the following ways:

- To delete a rule or an endpoint, click the **x** in the upper-right corner of the box.

Important

If you delete a rule that has child rules and endpoints, Route 53 also deletes all of the children.

- If you connect two rules to the same child rule or endpoint and you want to delete one of the connections, pause your cursor on the connection that you want to delete, and click the x for that connection.
9. When you're finished editing, choose **Save as new version**.
10. *Optional:* Specify the settings to create one or more policy records in one hosted zone by using the new traffic policy version. For more information, see [Values that you specify when you create or update a policy record \(p. 454\)](#). You can also create policy records later, either in the same hosted zone or in additional hosted zones.

If you don't want to create policy records now, choose **Skip this step**, and the console displays the list of traffic policies and policy records that you have created by using the current AWS account.

11. If you specified settings for policy records in the preceding step, choose **Create policy record**.

Creating a traffic policy by importing a JSON document

You can create a new traffic policy or a new version of an existing traffic policy by importing a document in JSON format that describes all of the endpoints and rules that you want to include in the traffic policy. For information about the format of the JSON document and several examples that you can copy and revise, see [Traffic policy document format](#) in the *Amazon Route 53 API Reference*.

The easiest way to get the JSON-formatted document for an existing traffic policy version is to use the `get-traffic-policy` command in the AWS CLI. For more information, see [get-traffic-policy](#) in the *AWS CLI Command Reference*.

To create a traffic policy by importing a JSON document

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. To create a new traffic policy by importing a JSON document, perform the following steps:
 - a. In the navigation pane, choose **Traffic policies**.
 - b. Choose **Create traffic policy**.
 - c. On the **Name policy** page, specify the applicable values. For more information, see [Values that you specify when you create a traffic policy \(p. 444\)](#).
 - d. Skip to step 4.
3. To create a new version of an existing traffic policy by importing a JSON document, perform the following steps:
 - a. In the navigation pane, choose **Traffic policies**.
 - b. Choose the name of the traffic policy that you want to base the new version on.
 - c. In the **Traffic policy versions** table, select the check box for the version that you want to base the new version on.
 - d. Choose **Edit policy as new version**.
 - e. On the **Update description** page, enter a description for the new version.
 - f. Skip to step 4.
4. Choose **Next**.
5. Choose **Import traffic policy**.
6. Enter a new traffic policy, paste an example traffic policy, or paste an existing traffic policy.
7. Choose **Import traffic policy**.

Viewing traffic policy versions and the associated policy records

You can view all of the versions that you've created for a traffic policy as well as all of the policy records that you've created by using each of the versions of the traffic policy.

To view traffic policy versions and the associated policy records

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Traffic policies**.
3. Choose the name of a traffic policy.
4. The top table lists all of the versions that you've created of a traffic policy. The table includes the following information:

Version number

The number of each version of a traffic policy that you've created. If you choose the version number, the console displays the configuration for that version.

Number of policy records

The number of policy records that you've created by using this traffic policy version.

DNS type

The DNS type that you specified when you created the traffic policy version.

Version description

The description that you specified when you created the traffic policy version.

5. The bottom table lists all of the policy records that you've created by using the traffic policy versions in the top table. The table includes the following information:

Policy record DNS name

The DNS names that you've associated the traffic policy with.

Status

Possible values include the following:

Applied

Route 53 has finished creating or updating a policy record and the corresponding records.

Creating

Route 53 is creating the records for a new policy record.

Updating

You have updated a policy record and Route 53 is in the process of creating a new group of records that will replace the existing group of records for the specified DNS name.

Deleting

Route 53 is in the process of deleting a policy record and the associated records.

Failed

Route 53 wasn't able to create or update the policy record and the associated records.

Version used

API Version 2013-04-01

Indicates the version of the traffic policy that you used to create the policy record.

DNS type

The DNS type of all of the records that Route 53 created for this policy record. When you edit a policy record, you must specify a traffic policy version that has the same DNS type as the DNS type for the policy record that you're editing.

TTL (in seconds)

The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you pay less for Route 53 service because recursive resolvers send requests to Route 53 less often. However, it takes longer for changes to the records (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods instead of asking Route 53 for the latest information.

Deleting traffic policy versions and traffic policies

To delete a traffic policy, you must delete all of the versions (including the original) that you've created for the traffic policy. In addition, to delete a traffic policy version, you must delete all of the policy records that you created by using the traffic policy version.

Important

If you delete policy records that Amazon Route 53 is using to respond to DNS queries, Route 53 will stop responding to queries for the corresponding DNS names. For example, if Route 53 is using the policy record for www.example.com to respond to DNS queries for www.example.com and you delete the policy record, your users will not be able to access your website or web application by using the domain name www.example.com.

To delete traffic policy versions and, optionally, a traffic policy, perform the following procedure:

To delete traffic policy versions and a traffic policy

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Traffic policies**.
3. Choose the name of the traffic policy for which you want to delete traffic policy versions and that, optionally, you want to delete completely.
4. If the traffic policy versions that you want to delete in the top table appear in the **Version used** column in the bottom table, select the check boxes for the corresponding policy records in the bottom table.

For example, if you want to delete version 3 of a traffic policy but you created one of the policy records in the bottom table by using version 3, select the check box for that policy record.

5. Choose **Delete policy records**.
6. Choose the refresh button for the bottom table to refresh the display until the policy records that you deleted no longer appear in the table.
7. In the top table, select the check boxes for the traffic policy versions that you want to delete.
8. Choose **Delete version**.
9. If you deleted all traffic policy versions in the preceding step and you want to delete the traffic policy, too, choose the refresh button for the top table to refresh the display until the table is empty.
10. In the navigation pane, choose **Traffic policies**.
11. In the list of traffic policies, select the check box for the traffic policy that you want to delete.
12. Choose **Delete traffic policy**.

Creating and managing policy records

To route internet traffic to the resources that you specified when you created a [traffic policy](#), you create one or more policy records. Each policy record identifies the hosted zone where you want to create the policy record and the domain or subdomain name that you want to route traffic for. For example, if you want to route traffic for `www.example.com`, you specify the hosted zone ID for the `example.com` hosted zone, and you specify `www.example.com` for the **Policy record DNS name**.

If you want to use the same traffic policy to route traffic for more than one domain or subdomain name, you have two options:

- You can create a policy record for each domain or subdomain name.
- You can create one policy record and then create CNAME or alias records that refer to the policy record.

For example, if you want to use the same traffic policy for `example.com`, `example.net`, and `example.org`, you can do either of the following:

- Create one policy record for each of them.
- Create a policy record for one of them and then create CNAME records in the hosted zones for the other two. In the two CNAME records, you specify the record name that you created a policy record for.

If you want to use the same traffic policy for a domain and its subdomains, such as `example.com` and `www.example.com`, you can create a policy record for one name and then create alias records for the rest. For example, you can create a policy record for `example.com` and then create an alias record for `www.example.com` that has the `example.com` record as the alias target.

Note

There's a monthly charge for each policy record that you create. If you want to use the same traffic policy for multiple domain or subdomain names, you can use CNAME or alias records to reduce your charges:

- If you create one policy record and one or more CNAME records that refer to the policy record, you pay only for the policy record and for DNS queries for the CNAME records.
- If you create one policy record and one or more alias records in the same hosted zone that refer to the policy record, you pay only for the policy record and for DNS queries for the alias records.

Topics

- [Creating policy records \(p. 453\)](#)
- [Values that you specify when you create or update a policy record \(p. 454\)](#)
- [Updating policy records \(p. 455\)](#)
- [Deleting policy records \(p. 455\)](#)

Creating policy records

To create a policy record, perform the following procedure.

Important

For each policy record that you create, you incur a monthly charge. If you later delete the policy record, the charge is prorated. For more information, see the section "Traffic Flow" on the [Amazon Route 53 Pricing](#) page.

To create a policy record

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Policy records**.
3. On the **Policy records** page, choose **Create policy records**.
4. On the **Create policy records** page, specify the applicable values. For more information, see [Values that you specify when you create or update a policy record \(p. 454\)](#).
5. Choose **Create policy records**.
6. If you want to create policy records in another hosted zone, repeat steps 3 through 5.

Values that you specify when you create or update a policy record

When you create or update a policy record, you specify the following values

- [Traffic policy](#)
- [Version](#)
- [Hosted zone](#)
- [Policy record DNS name](#)
- [TTL](#)

Traffic policy

Choose the traffic policy whose configuration you want to use for this policy record.

Version

Choose the version of the traffic policy whose configuration you want to use for this policy record.

If you're updating an existing policy record, you must choose a version for which the DNS type matches the current DNS type of the policy record. For example, if the DNS type of the policy record is A, you must choose a version for which the DNS type is A.

Hosted zone

Choose the hosted zone in which you want to create a policy record by using the specified traffic policy and version. You can't change the value of **Hosted zone** after you create a policy record.

Policy record DNS name

When you're creating a policy record, enter the domain name or subdomain name for which you want Route 53 to respond to DNS queries by using the configuration in the specified traffic policy and version.

To use the same configuration for more than one domain name or subdomain name in the specified hosted zone, choose **Add another policy record**, and enter the applicable domain name or subdomain name and TTL.

You can't change the value of **Policy record DNS name** after you create a policy record.

TTL (in seconds)

Enter the amount of time, in seconds, that you want DNS recursive resolvers to cache information about this record. If you specify a longer value (for example, 172800 seconds, or two days), you pay less for Route 53 service because recursive resolvers send requests to Route 53 less often. However, it takes longer for changes to the records (for example, a new IP address) to take effect because

recursive resolvers use the values in their cache for longer periods instead of asking Route 53 for the latest information.

Updating policy records

To update the settings in a policy record, perform the following procedure.

To update a policy record

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Policy records**.
3. On the **Policy records** page, select the check box for the policy record that you want to update, and choose **Edit policy record**.
4. On the **Edit policy record** page, specify the applicable values. For more information, see [Values that you specify when you create or update a policy record \(p. 454\)](#).
5. Choose **Edit policy record**.
6. If you want to update another policy record, repeat steps 3 through 5.

Deleting policy records

To delete policy records, perform the following procedure.

Important

If you delete policy records that Amazon Route 53 is using to respond to DNS queries, Route 53 will stop responding to queries for the corresponding DNS names. For example, if Route 53 is using the policy record for www.example.com to respond to DNS queries for www.example.com and you delete the policy record, your users will not be able to access your website or web application by using the domain name www.example.com.

To delete a policy record

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Policy records**.
3. On the **Policy records** page, select the check boxes for the policy records that you want to delete, and choose **Delete policy record**.

Configuring DNSSEC signing in Amazon Route 53

Domain Name System Security Extensions (DNSSEC) signing lets DNS resolvers validate that a DNS response came from Amazon Route 53 and has not been tampered with. When you use DNSSEC signing, every response for a hosted zone is signed using public key cryptography.

In this chapter, we explain how to enable DNSSEC signing for Route 53, how to work with key-signing keys (KSKs), and how to troubleshoot issues. You can work with DNSSEC signing in the AWS Management Console or programmatically with the API. For more information about using the CLI or SDKs to work with Route 53, see [Setting up Amazon Route 53 \(p. 13\)](#).

Before you enable DNSSEC signing, note the following:

- To help prevent a zone outage and avoid problems with your domain becoming unavailable, you must quickly address and resolve DNSSEC errors. We strongly recommend that you set up a CloudWatch alarm that alerts you whenever a `DNSSECInternalFailure` or

`DNSSECKeySigningKeysNeedingAction` error is detected. For more information, see [Monitoring hosted zones using Amazon CloudWatch \(p. 628\)](#).

- There are two kinds of keys in DNSSEC: a key-signing key (KSK) and a zone-signing key (ZSK). In Route 53 DNSSEC signing, each KSK is based on an [asymmetric customer managed key](#) in AWS KMS that you own. You are responsible for KSK management, which includes rotating it if needed. ZSK management is performed by Route 53.
- When you enable DNSSEC signing for a hosted zone, Route 53 limits the TTL to one week. If you set a TTL of more than one week for records in the hosted zone, you don't get an error. However, Route 53 enforces a TTL of one week for the records. Records that have a TTL of less than one week and records in other hosted zones that do not have DNSSEC signing enabled are not affected.
- When you use DNSSEC signing, multi-vendor configurations are not supported.
- It can be helpful to set up IAM permissions to allow another user, besides the zone owner, to add or remove records in the zone. For example, a zone owner can add a KSK and enable signing, and might also be responsible for key rotation. However, someone else might be responsible for working with other records for the hosted zone. For an example IAM policy, see [Example permissions for a domain record owner \(p. 583\)](#).

Topics

- [Enabling DNSSEC signing and establishing a chain of trust \(p. 456\)](#)
- [Disabling DNSSEC signing \(p. 462\)](#)
- [Working with customer managed keys for DNSSEC \(p. 465\)](#)
- [Working with key-signing keys \(KSKs\) \(p. 466\)](#)
- [KMS key and ZSK management in Route 53 \(p. 468\)](#)
- [DNSSEC proofs of nonexistence in Route 53 \(p. 468\)](#)
- [Troubleshooting DNSSEC signing \(p. 469\)](#)

Enabling DNSSEC signing and establishing a chain of trust

The incremental steps apply to the hosted zone owner and the parent zone maintainer. This can be the same person, but if not, the zone owner should notify and work with the parent zone maintainer.

We recommend following the steps in this article to have your zone signed and included in the chain of trust. The following steps will minimize the risk of onboarding onto DNSSEC.

There are three steps to take to enable DNSSEC signing, as described in the following sections.

Topics

- [Step 1: Prepare for enabling DNSSEC signing \(p. 456\)](#)
- [Step 2: Enable DNSSEC signing and create a KSK \(p. 458\)](#)
- [Step 3: Establish chain of trust \(p. 459\)](#)

Step 1: Prepare for enabling DNSSEC signing

The preparation steps help you minimize the risk of onboarding to DNSSEC by monitoring zone availability and lowering wait times between enabling signing and the insertion of the Delegation Signer (DS) record.

To prepare for enabling DNSSEC signing

1. Monitor zone availability.

You can monitor the zone for the availability of your domain names. This can help you address any issues that might warrant rolling a step back after you enable DNSSEC signing. You can monitor for your domain names with most traffic by using query logging. For more information about setting up query logging, see [Monitoring Amazon Route 53 \(p. 615\)](#).

The monitoring can be done through a shell script, or through a third party service. It shouldn't, however, be the only signal to determine if a rollback is required. You might also get feedback from your customers due to a domain not being available.

2. Lower the zone's maximum TTL.

The zone's maximum TTL is the longest TTL record in the zone. In the following example zone, the zone's maximum TTL is 1 day (86400 seconds).

Name	TTL	Record class	Record type	Record data
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 2002022401 10800 15 604800 300
example.com.	900	IN	NS	ns1.example.com.
route53.example.com	86400	IN	TXT	some txt record

Lowering the zone's maximum TTL will help reduce the wait time between enabling signing and the insertion of the Delegation Signer (DS) record. We recommend lowering the zone's maximum TTL to 1 hour (3600 seconds). This allows you to roll back after only an hour if any resolver has problems with caching signed records.

Rollback: undo the TTL changes.

3. Lower the SOA TTL and SOA minimum field.

The SOA minimum field is the last field in the SOA record data. In the following example SOA record, the minimum field has the value of 5 minutes (300 seconds).

Name	TTL	Record class	Record type	Record data
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 2002022401 10800 15 604800 300

The SOA TTL and SOA minimum field determines how long resolvers remember negative answers. After you enable signing, Route 53 name servers start returning NSEC records for negative answers. The NSEC contains information that resolvers might use to synthesize a negative answer. If you have to roll back because the NSEC information caused a resolver to assume a negative answer for a name, then you only have to wait for the maximum of the SOA TTL and SOA minimum field for the resolver to stop the assumption.

Rollback: undo the SOA changes.

4. Make sure the TTL and SOA minimum field changes are effective.

Use [GetChange](#) to make sure your changes so far have been propagated to all Route 53 DNS servers.

Step 2: Enable DNSSEC signing and create a KSK

You can enable DNSSEC signing and create a key-signing key (KSK) by using AWS CLI or on the Route 53 console.

- [CLI \(p. 458\)](#)
- [Console \(p. 458\)](#)

When you provide or create a customer managed KMS key, there are several requirements. For more information, see [Working with customer managed keys for DNSSEC \(p. 465\)](#).

CLI

You can use a key that you already have, or create one by running an AWS CLI command like the following using your own values for `hostedzone_id`, `cmk_arn`, `ksk_name`, and `unique_string` (to make the request unique):

```
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
```

For more information about customer managed keys, see [Working with customer managed keys for DNSSEC \(p. 465\)](#). See also [CreateKeySigningKey](#).

To enable DNSSEC signing, run an AWS CLI command like the following, using your own value for the `hostedzone_id`:

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
--hosted-zone-id $hostedzone_id
```

For more information, see [enable-hosted-zone-dnssec](#) and [EnableHostedZoneDNSSEC](#).

Console

To enable DNSSEC signing and create a KSK

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone that you want to enable DNSSEC signing for.
3. On the **DNSSEC signing** tab, choose **Enable DNSSEC signing**.

Note

If the option in this section is **Disable DNSSEC signing**, you have already completed the first step in enabling DNSSEC signing. Be sure that you establish, or that there already exists, a chain of trust for the hosted zone for DNSSEC, and then you're done. For more information, see [Step 3: Establish chain of trust \(p. 459\)](#).

4. In the **Key-signing key (KSK) creation** section, choose **Create new KSK**, and under **Provide KSK name**, enter a name for the KSK that Route 53 will create for you. The name can include numbers, letters, and underscores (_). It must be unique.

5. Under **Customer managed CMK**, choose the customer managed key for Route 53 to use when it creates the KSK for you. You can use an existing customer managed key that applies to DNSSEC signing, or create a new customer managed key.

When you provide or create a customer managed key, there are several requirements. For more information, see [Working with customer managed keys for DNSSEC \(p. 465\)](#).

6. Enter the alias for an existing customer managed key. If you want to use a new customer managed key, enter an alias for the customer managed key, and Route 53 will create one for you.

Note

If you choose to have Route 53 create a customer managed key, be aware that separate charges apply for each customer managed key. For more information, see [AWS Key Management Service pricing](#).

7. Choose **Enable DNSSEC signing**.

After you enable zone signing, complete the following steps (whether you used the console or the CLI):

1. Ensure zone signing is effective.

Use the Id from the `EnableHostedZoneDNSSEC()` call to run [GetChange](#) to make sure that all Route 53 DNS Servers are signing responses (status = `INSYNC`).

2. Wait for at least the previous zone's maximum TTL.

Wait for resolvers to flush all unsigned records from their cache. To achieve this you should wait for at least the previous zone's maximum TTL. In the `example.com` zone above, the wait time would be 1 day.

3. Monitor for reports of customer issues.

After you have enabled zone signing, your customers might start seeing issues related to network devices and resolvers. The recommended monitoring period is 2 weeks.

The following are examples of issues that you might see:

- Some network devices can limit DNS response size to under 512 bytes, which is too small for some signed responses. These network devices should be reconfigured to allow larger DNS response sizes.
- Some network devices do a deep inspection on DNS responses and strips certain records it doesn't understand, like the ones used for DNSSEC. These devices should be reconfigured.
- Some customers' resolvers claim that they can accept a larger UDP response than their network supports. You can test your network capability and configure your resolvers appropriately. For more information see, [DNS Reply Size Test Server](#).

Rollback: call `DisableHostedZoneDNSSEC` then rollback the steps in [Step 1: Prepare for enabling DNSSEC signing \(p. 456\)](#).

Step 3: Establish chain of trust

After you enable DNSSEC signing for a hosted zone in Route 53, establish a chain of trust for the hosted zone to complete your DNSSEC signing setup. You do this by creating a Delegation Signer (DS) record in the *parent* hosted zone, for your hosted zone, using the information that Route 53 provides. Depending on where your domain is registered, you add the record to the parent hosted zone in Route 53 or at another domain registrar.

To establish a chain of trust for DNSSEC signing

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone that you want to establish a DNSSEC chain of trust for. You must enable DNSSEC signing first.
3. On the **DNSSEC signing** tab, under **DNSSEC signing**, choose **View information to create DS record**.

Note

If you don't see **View information to create DS record** in this section, then you must enable DNSSEC signing before you establish the chain of trust. Choose **Enable DNSSEC signing** and complete the steps as described in [Step 2: Enable DNSSEC signing and create a KSK \(p. 458\)](#), and then return to these steps to establish the chain of trust.

4. Under **Establish a chain of trust**, choose either **Route 53 registrar** or **Another domain registrar**, depending on where your domain is registered.
5. Use the provided values from step 3 to create a DS record for the parent hosted zone in Route 53. If your domain is not hosted at Route 53, use the provided values to create a DS record at your domain registrar website.
 - If the parent zone is both registered and managed through Route 53, follow these steps:

Make sure that you configure the correct signing algorithm (ECDSAP256SHA256 and type 13) and digest algorithm (SHA-256 and type 2).

If Route 53 is your registrar, do the following in the Route 53 console:

1. Note the **Key type**, **Signing algorithm**, and **Public key** values. In the navigation pane, choose **Registered domains**.
2. Select a domain, and then, next to **DNSSEC status**, choose **Manage keys**.
3. In the **Manage DNSSEC keys** dialog box, choose the appropriate **Key type** and **Algorithm** for the **Route 53 registrar** from the dropdown menus.
4. Copy the **Public key** for the Route 53 registrar. In the **Manage DNSSEC keys** dialog box, paste the value into the **Public key** box.
5. Choose **Add**.

Route 53 will add the DS record to the parent zone from the public key. For example, if your domain is `example.com`, the DS record is added to the `.com` DNS zone.

- If the parent zone is hosted on Route 53 or another registry, contact the parent zone owner to follow these instructions:

To make sure the following steps go smoothly, introduce a low DS TTL to the parent zone. We recommend setting the DS TTL to 5 minutes (300 seconds) for faster recovery if you need to roll your changes back.

- If your parent zone is administered by another registry, contact your registrar to introduce the DS record for your zone. Typically you will not be able to adjust the TTL of the DS record.
- If your parent zone is hosted on Route 53, contact the parent zone owner to introduce the DS record for your zone.

Provide the `$ds_record_value` to the parent zone owner. You can get it by clicking on the **View Information to create DS record** in the console and copying the **DS record** field, or by calling [GetDNSSEC API](#) and retrieving the value of the 'DSRecord' field:

```
aws --region us-east-1 route53 get-dnssec
--hosted-zone-id $hostedzone_id
```

The parent zone owner can insert the record through the Route 53 console or CLI.

- To insert the DS record by using AWS CLI, the parent zone owner creates and names a JSON file similar to the following example. The parent zone owner might name the file something like `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"  
                        }  
                    ]  
                }  
            }  
        ]  
    }  
}
```

Then run the following command:

```
aws --region us-east-1 route53 change-resource-record-sets  
    --cli-input-json file://inserting_ds.json
```

- To insert the DS record by using the console,

Open the Route 53 console at <https://console.aws.amazon.com/route53/>.

In the navigation pane, choose **Hosted zones**, the name of your hosted zone and then **Create record** button. Make sure you choose Simple routing for the **Routing policy**.

In the **Record name** field enter the same name as the `$zone_name`, select DS from the **Record type** drop-down, and enter the value of `$ds_record_value` into the **Value** field, and choose **Create records**.

Rollback: remove the DS from the parent zone, wait for the DS TTL, and then roll back the steps for establishing trust. If the parent zone is hosted on Route 53, the parent zone owner can change the Action from UPSERT to DELETE in the JSON file, and re-run the example CLI above.

6. Wait for the updates to propagate, based on the TTL for your domain records.

If the parent zone is on Route 53 DNS service, the parent zone owner can confirm full propagation through the [GetChange API](#).

Otherwise, you can periodically probe the parent zone for the DS record, and then wait another 10 minutes afterwards to increase the probability of the DS record insertion being fully propagated. Do note that some registrars have scheduled DS insertion, for example, once a day.

When you introduce the Delegation Signer (DS) record in the parent zone, the validated resolvers that have picked up the DS will start validating responses from the zone.

To make sure the steps for establishing trust go smoothly, complete the following:

1. Find the maximum NS TTL.

There are 2 sets of NS records associated with your zones:

- The delegation NS record — this is the NS record for your zone held by the parent zone. You can find this by running the following Unix commands (if your zone is example.com, the parent zone is com):

```
dig -t NS com
```

Pick one of the NS records and then run the following:

```
dig @one of the NS records of your parent zone -t NS example.com
```

For example:

```
dig @b.gtld-servers.net. -t NS example.com
```

- The in-zone NS record — this is the NS record in your zone. You can find this by running the following Unix command:

```
dig @one of the NS records of your zone -t NS example.com
```

For example:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

Note the maximum TTL for both zones.

2. Wait for the maximum NS TTL.

Prior to the DS insertion, resolvers are getting a signed response, but aren't validating the signature. When the DS record is inserted, resolvers will not see it until the NS record for the zone expires. When resolvers re-fetch the NS record, the DS record will then be also returned.

If your customer is running a resolver on a host with an out of sync clock, make sure the clock is within 1 hour of the correct time.

After completing this step, all DNSSEC-aware resolvers will validate your zone.

3. Observe name resolution.

You should observe that there are no issues with resolvers validating your zone. Make sure you also account for the time needed for your customers to report problems to you.

We recommend monitoring for up to 2 weeks.

4. (Optional) Lengthen the DS and NS TTLs.

If you are satisfied with the setup, you can save the TTL and SOA changes you made. Note that Route 53 limits the TTL to 1 week for signed zones. For more information, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

If you can change the DS TTL, we recommend that you set it to 1 hour.

Disabling DNSSEC signing

The steps for disabling DNSSEC signing in Route 53 vary, depending on the chain of trust that your hosted zone is part of.

For example, your hosted zone might have a parent zone that has a Delegation Signer (DS) record, as part of a chain of trust. Your hosted zone might also be itself a parent zone for child zones that have enabled DNSSEC signing, which is another part of the chain of trust. Investigate and determine the full chain of trust for your hosted zone before you take the steps to disable DNSSEC signing.

The chain of trust for your hosted zone that enables DNSSEC signing must be carefully undone as you disable signing. To remove your hosted zone from the chain of trust, you remove all DS records that are in place for the chain of trust that includes this hosted zone. This means that you must do the following, in order:

1. Remove any DS records that this hosted zone has for child zones that are part of a chain of trust.
2. Remove the DS record from the parent zone. Skip this step if you have an island of trust (there are no DS records in the parent zone and no DS records for child zones in this zone).

The following incremental steps allow you to monitor the effectiveness of the individual steps to avoid DNS availability issues in your zone.

To disable DNSSEC signing

1. Monitor zone availability.

You can monitor the zone for the availability of your domain names. This can help you address any issues that might warrant rolling a step back after you enable DNSSEC signing. You can monitor for your domain names with most traffic by using query logging. For more information about setting up query logging, see [Monitoring Amazon Route 53 \(p. 615\)](#).

The monitoring can be done through a shell script, or through a paid service. It shouldn't, however, be the only signal to determine if a rollback is required. You might also get feedback from your customers due to a domain not being available.

2. Find the current DS TTL.

You can find the DS TTL by running the following Unix command:

```
dig -t DS example.com example.com
```

3. Find the maximum NS TTL.

There are 2 sets of NS records associated with your zones:

- The delegation NS record — this is the NS record for your zone held by the parent zone. You can find this by running the following Unix commands:

First find the NS of your parent zone (if your zone is example.com, the parent zone is com):

```
dig -t NS com
```

Pick one of the NS records and then run the following:

```
dig @one of the NS records of your parent zone -t NS example.com
```

For example:

```
dig @b.gtld-servers.net. -t NS example.com
```

- The in-zone NS record — this is the NS record in your zone. You can find this by running the following Unix command:

```
dig @one of the NS records of your zone -t NS example.com
```

For example:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

Note the maximum TTL for both zones.

4. Remove the DS record from the parent zone.

Contact the parent zone owner to remove the DS record.

Rollback: re-insert the DS TTL, confirm DS insertion is effective, and wait for the maximum NS (not DS) TTL before all resolvers will start validating again.

5. Confirm the DS removal is effective.

If the parent zone is on Route 53 DNS service, the parent zone owner can confirm full propagation through the [GetChange API](#).

Otherwise, you can periodically probe the parent zone for the DS record, and then wait another 10 minutes afterwards to increase the probability of the DS record removal being fully propagated. Do note that some registrars have scheduled DS removal, for example once a day.

6. Wait for the DS TTL.

Wait until all resolvers have expired the DS record from their caches.

7. Disable DNSSEC signing and deactivate the key-signing key (KSK).

- [CLI \(p. 464\)](#)
- [Console \(p. 464\)](#)

CLI

Call [DisableHostedZoneDNSSEC](#) and [DeactivateKeySigningKey](#) APIs.

For example:

```
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

To disable DNSSEC signing

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone that you want to disable DNSSEC signing for.
3. On the **DNSSEC signing** tab, choose **Disable DNSSEC signing**.
4. On the **Disable DNSSEC signing** page, choose one of the following options, depending on your scenario for the zone that you're disabling DNSSEC signing for.
 - **Parent zone only** — This zone has a parent zone with a DS record. In this scenario, you must remove the parent zone's DS record.
 - **Child zones only** — This zone has a DS record for a chain of trust with one or more child zones. In this scenario, you must remove the zone's DS records.
 - **Parent and child zones** — This zone has both a DS record for a chain of trust with one or more child zones *and* a parent zone with a DS record. In this scenario, do the following, in order:
 - a. Remove the zone's DS records.
 - b. Remove the parent zone's DS record.

If you have an island of trust, you can skip this step.

5. Determine what the TTL is for each DS record that you remove in Step 4. Make sure that the longest TTL period has expired.
6. Select the check box to confirm that you have followed the steps in order.
7. Type *disable* in the field, as shown, and then choose **Disable**.

To deactivate the key-signing key (KSK)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone that you want to deactivate the key-signing key (KSK) for.
3. In the **Key-signing keys (KSKs)** section, choose the KSK you want to deactivate, and under **Actions**, choose **Edit KSK**, set **KSK status** to **Inactive**, and then choose **Save KSK**.

Rollback: call [ActivateKeySigningKey](#) and [EnableHostedZoneDNSSEC](#) APIs.

For example:

```
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. Confirm disabling zone signing is effective.

Use the Id from the `EnableHostedZoneDNSSEC()` call to run [GetChange](#) to make sure that all Route 53 DNS Servers have stopped signing responses (status = `INSYNC`).

9. Observe name resolution.

You should observe that there are no issues resulting in resolvers validating your zone. Allow 1-2 weeks to also account for the time needed for your customers to report problems to you.

10. (Optional) Clean up.

If you will not re-enable signing, you can clean up the KSKs through [DeleteKeySigningKey](#) and delete the corresponding customer managed key to save costs.

Working with customer managed keys for DNSSEC

When you enable DNSSEC signing in Amazon Route 53, Route 53 creates a key-signing key (KSK) for you. To create a KSK, Route 53 must use a customer managed key in AWS Key Management Service that supports DNSSEC. This section describes the details and requirements for the customer managed key that are helpful to know as you work with DNSSEC.

Keep the following in mind when you work with customer managed keys for DNSSEC:

- The customer managed key that you use with DNSSEC signing must be in the US East (N. Virginia) Region.

- The customer managed key must be an [asymmetric customer managed key](#) with an [ECC_NIST_P256 key spec](#). These customer managed keys are used only for signing and verification. For help creating an asymmetric customer managed key, see [Creating asymmetric customer managed keys](#) in the AWS Key Management Service Developer Guide. For help finding the cryptographic configuration of an existing customer managed key, see [Viewing the cryptographic configuration of customer managed keys](#) in the AWS Key Management Service Developer Guide.
- If you create a customer managed key yourself to use with DNSSEC in Route 53, you must include specific key policy statements that give Route 53 the required permissions. Route 53 must be able to access your customer managed key so that it can create a KSK for you. For more information, see [Route 53 customer managed key permissions required for DNSSEC signing \(p. 583\)](#).
- Route 53 can create a customer managed key for you in AWS KMS to use with DNSSEC signing without additional AWS KMS permissions. However, you must have specific permissions if you want to edit the key after it's created. The specific permissions that you must have are the following: `kms:UpdateKeyDescription`, `kms:UpdateAlias`, and `kms:PutKeyPolicy`.
- Be aware that separate charges apply for each customer managed key that you have, whether you create the customer managed key or Route 53 creates it for you. For more information, see [AWS Key Management Service pricing](#).

Working with key-signing keys (KSKs)

When you enable DNSSEC signing, Route 53 creates a key-signing key (KSK) for you. You can have up to two KSKs per hosted zone in Route 53. After you enable DNSSEC signing, you can add, remove, or edit your KSKs.

Note the following when you work with your KSKs:

- Before you can delete a KSK, you must edit the KSK to set its status to **Inactive**.
- When DNSSEC signing is enabled for a hosted zone, Route 53 limits the TTL to one week. If you set a TTL for records in the hosted zone to more than one week, you don't get an error, but Route 53 enforces a TTL of one week.
- To help prevent a zone outage and avoid problems with your domain becoming unavailable, you must quickly address and resolve DNSSEC errors. We strongly recommend that you set up a CloudWatch alarm that alerts you whenever a `DNSSECInternalFailure` or `DNSSECKeySigningKeysNeedingAction` error is detected. For more information, see [Monitoring hosted zones using Amazon CloudWatch \(p. 628\)](#).
- The KSK operations described in this section allow you to rotate your zone's KSKs. For more information and a step-by-step example, see [DNSSEC Key Rotation](#) in the blog post [Configuring DNSSEC signing and validation with Amazon Route 53](#).

To work with KSKs in the AWS Management Console, follow the guidance in the following sections.

Add a key-signing key (KSK)

When you enable DNSSEC signing, Route 53 creates a key-signing (KSK) for you. You can also add KSKs separately. You can have up to two KSKs per hosted zone in Route 53.

When you create a KSK, you must provide or request Route 53 to create a customer managed customer managed key to use with the KSK. When you provide or create a customer managed customer managed key, there are several requirements. For more information, see [Working with customer managed keys for DNSSEC \(p. 465\)](#).

Follow these steps to add a KSK in the AWS Management Console.

To add a KSK

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone.
3. On the **DNSSEC signing** tab, under **Key-signing keys (KSKs)**, choose **Switch to advanced view**, and then, under **Actions**, choose **Add KSK**.
4. Under **KSK**, enter a name for the KSK that Route 53 will create for you. The name can include numbers, letters, and underscores (_). It must be unique.
5. Enter the alias for a customer managed customer managed key that applies to DNSSEC signing, or enter an alias for a new customer managed customer managed key that Route 53 will create for you.

Note

If you choose to have Route 53 create a customer managed key, be aware that separate charges apply for each customer managed key. For more information, see [AWS Key Management Service pricing](#).

6. Choose **Create KSK**.

Edit a key-signing key (KSK)

You can edit the status of a KSK to be **Active** or **Inactive**. When a KSK is active, Route 53 uses that KSK for DNSSEC signing. Before you can delete a KSK, you must edit the KSK to set its status to **Inactive**.

Follow these steps to edit a KSK in the AWS Management Console.

To edit a KSK

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone.
3. On the **DNSSEC signing** tab, under **Key-signing keys (KSKs)**, choose **Switch to advanced view**, and then, under **Actions**, choose **Edit KSK**.
4. Make the desired updates to the KSK, and then choose **Save**.

Delete a key-signing key (KSK)

Before you can delete a KSK, you must edit the KSK to set its status to **Inactive**.

One reason that you might delete a KSK is as part of routine key rotation. It's a best practice to rotate cryptographic keys periodically. Your organization might have standard guidance for how often to rotate keys.

Follow these steps to delete a KSK in the AWS Management Console.

To delete a KSK

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**, and then choose a hosted zone.
3. On the **DNSSEC signing** tab, under **Key-signing keys (KSKs)**, choose **Switch to advanced view**, and then under **Actions**, choose **Delete KSK**.
4. Follow the guidance to confirm deleting the KSK.

KMS key and ZSK management in Route 53

This section describes the current practice Route 53 uses for your DNSSEC signing enabled zones.

Note

Route 53 uses the following rule which might change. Any future changes will not reduce your zone's or Route 53's security posture.

How Route 53 uses the AWS KMS associated with your KSK

In DNSSEC, the KSK is used to generate the resource record signature (RRSIG) for the DNSKEY resource record set. All ACTIVE KSKs are used in the RRSIG generation. Route 53 generates an RRSIG by calling the [Sign AWS KMS API](#) on the associated KMS key. For more information, see [Sign](#) in the [AWS KMS API guide](#). These RRSIGs do not count towards the zone's resource record set limit.

RRSIG has an expiration. To prevent the RRSIGs from expiring, the RRSIGs are refreshed regularly by regenerating them every one to seven days.

The RRSIGs are also refreshed every time you call any of these APIs:

- [ActivateKeySigningKey](#)
- [CreateKeySigningKey](#)
- [DeactivateKeySigningKey](#)
- [DeleteKeySigningKey](#)
- [DisableHostedZoneDNSSEC](#)
- [EnableHostedZoneDNSSEC](#)

Every time Route 53 performs a refresh, we generate 15 RRSIGs to cover the next few days in case the associated KMS key becomes inaccessible. For KMS key cost estimation, you can assume a once a day regular refresh. A KMS key might become inaccessible by inadvertent changes to the KMS key policy. Inaccessible KMS key will set the associated KSK's status to ACTION_NEEDED. We strongly recommend that you monitor this condition by setting up a CloudWatch alarm whenever a `DNSSECKeySigningKeysNeedingAction` error is detected because validating resolvers will start failing lookups after the last RRSIG expires. For more information, see [Monitoring hosted zones using Amazon CloudWatch \(p. 628\)](#).

How Route 53 manages your zone's ZSK

Each new hosted zone with DNSSEC signing enabled will have one ACTIVE zone signing key (ZSK). The ZSK is generated separately for each hosted zone and is owned by Route 53. The current key algorithm is ECDSAP256SHA256.

We will start performing regular ZSK rotation on the zone within 7–30 days of the start of signing. Currently, Route 53 uses the Pre-Publish Key Rollover method. For more information, see [Pre-Publish Zone Signing Key Rollover](#). This method will introduce another ZSK to the zone. The rotation will be repeated every 7–30 days.

Route 53 will suspend ZSK rotation if any of the zone's KSK is in ACTION_NEEDED status because Route 53 will not be able to regenerate the RRSIGs for DNSKEY resource record sets to account for the changes in the zone's ZSK. ZSK rotation will automatically resume after the condition is cleared.

DNSSEC proofs of nonexistence in Route 53

Note

Route 53 uses the following rule which might change. Any future changes will not reduce your zone's or Route 53's security posture.

There are three kinds of proof of nonexistence in DNSSEC:

- Proof of nonexistence of a record matching the query name.
- Proof of nonexistence of a type matching the query type.
- Proof of existence of a wildcard record used to generate the record in response.

Route 53 implements the proof of nonexistence of a record matching the query name using the BL method. For more information, see [BL](#). It's a method that produces a compact representation of the proof and prevents zone walking.

In cases where there is a record matching the query name but not the query type (such as querying for web.example.com/AAAA but there is only web.example.com/A present), we return a minimal NSEC (next secure) record containing all supported resource record types.

When Route 53 synthesizes an answer from a wildcard record, the response will not be accompanied with an NSEC record for the wildcard. Such NSEC record is used in some implementations, typically those performing offline signing, to prevent the resource record signatures (RRSIG) in the response from being re-used to spoof a different response. Route 53 uses online signing for non-DNSKEY to generate RRSIGs specific to the response which cannot be re-used for a different response.

Troubleshooting DNSSEC signing

The information in this section can help you address issues with DNSSEC signing, including with your key-signing keys (KSKs).

KSK status is **Action needed**

A KSK can change its status to **Action needed** (or ACTION_NEEDED in a [KeySigningKey](#) status), when Route 53 DNSSEC loses access to a corresponding AWS KMS key (due to a change in permissions or AWS KMS key deletion).

If the status of a KSK is **Action needed**, it means that eventually it'll cause a zone outage for clients using DNSSEC validating resolvers and you must act fast to prevent a production zone becoming unresolvable.

To correct the problem, make sure that the customer managed key that your KSK is based on is enabled and has the correct permissions. For more information about the required permissions, see [Route 53 customer managed key permissions required for DNSSEC signing \(p. 583\)](#).

After you have fixed the KSK, activate it again by using the console or the AWS CLI, as described in [Step 2: Enable DNSSEC signing and create a KSK \(p. 458\)](#).

To prevent this issue in the future, consider adding an Amazon CloudWatch metric to track the state of the KSK as suggested in [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

KSK status is **Internal failure**

When a KSK has a status of **Internal failure** (or INTERNAL_FAILURE in a [KeySigningKey](#) status), you can't work with any other DNSSEC entities until the problem is resolved. You must take action before you can work with DNSSEC signing, including working with this KSK or your other KSK.

To correct the problem, try again to activate or deactivate the KSK.

To correct the problem when working with the APIs, try enabling signing ([EnableHostedZoneDNSSEC](#)) or disabling signing ([DisableHostedZoneDNSSEC](#)).

It's important that you correct **Internal failure** problems promptly. You can't make any other changes to the hosted zone until you correct the problem, except the operations to fix the **Internal failure**.

Using AWS Cloud Map to create records and health checks

If you want to route internet traffic or traffic within an Amazon VPC to application components or microservices, you can use AWS Cloud Map to automatically create records and, optionally, to create health checks. For more information, see the [AWS Cloud Map Developer Guide](#).

DNS constraints and behaviors

DNS messaging is subject to factors that affect how you create and use hosted zones and records. This section explains these factors.

Maximum response size

To comply with DNS standards, responses sent over UDP are no more than 512 bytes in size. Responses exceeding 512 bytes are truncated and the resolver must re-issue the request over TCP. If the resolver supports EDNS0 (as defined in [RFC 2671](#)), and advertises the EDNS0 option to Amazon Route 53, Route 53 permits responses up to 4096 bytes over UDP, without truncation.

Authoritative section processing

For successful queries, Route 53 appends name server (NS) records for the relevant hosted zone to the Authority section of the DNS response. For names that are not found (NXDOMAIN responses), Route 53 appends the start of authority (SOA) record (as defined in [RFC 1035](#)) for the relevant hosted zone to the Authority section of the DNS response.

Additional section processing

Route 53 appends records to the Additional section. If the records are known and appropriate, the service appends A or AAAA records for any target of an MX, CNAME, NS, or SRV record cited in the Answer section. For more information about these DNS record types, see [Supported DNS record types \(p. 382\)](#).

Resolving DNS queries between VPCs and your network

When you create a VPC using Amazon VPC, Route 53 Resolver automatically uses a Resolver on the VPC to answer DNS queries for local Amazon VPC domain names for EC2 instances (`ec2-192-0-2-44.compute-1.amazonaws.com`) and records in private hosted zones (`acme.example.com`). For all other domain names, Resolver performs recursive lookups against public name servers.

When you create a VPC, the Route 53 Resolver that is created by default, maps to a DNS server that runs on a reserved IP address for the VPC network range, plus 2. For example, the DNS Server on a `10.0.0.0/16` network is located at `10.0.0.2`. For VPCs with multiple IPv4 CIDR blocks, the DNS server IP address is located in the primary CIDR block. The DNS server does not reside within a specific subnet or Availability Zone in a VPC. For more information, see [DNS support for your VPC](#) and [Amazon DNS server](#) in the *Amazon Virtual Private Cloud User Guide*.

The Resolver additionally contains endpoints that you configure to answer DNS queries to and from your on-premises environment.

You also can integrate DNS resolution between Resolver and DNS resolvers on your network by configuring forwarding rules. *Your network* can include any network that is reachable from your VPC, such as the following:

- The VPC itself
- Another peered VPC
- An on-premises network that is connected to AWS with AWS Direct Connect, a VPN, or a network address translation (NAT) gateway

Before you start to forward queries, you create Resolver inbound and/or outbound endpoints in the connected VPC. These endpoints provide a path for inbound or outbound queries:

Inbound endpoint: DNS resolvers on your network can forward DNS queries to Route 53 Resolver via this endpoint

This allows your DNS resolvers to easily resolve domain names for AWS resources such as EC2 instances or records in a Route 53 private hosted zone. For more information, see [How DNS resolvers on your network forward DNS queries to Route 53 Resolver endpoints \(p. 473\)](#).

Outbound endpoint: Resolver conditionally forwards queries to resolvers on your network via this endpoint

To forward selected queries, you create Resolver rules that specify the domain names for the DNS queries that you want to forward (such as `example.com`), and the IP addresses of the DNS resolvers on your network that you want to forward the queries to. If a query matches multiple rules (`example.com`, `acme.example.com`), Resolver chooses the rule with the most specific match (`acme.example.com`) and forwards the query to the IP addresses that you specified in that rule. For more information, see [How Route 53 Resolver endpoint forwards DNS queries from your VPCs to your network \(p. 473\)](#).

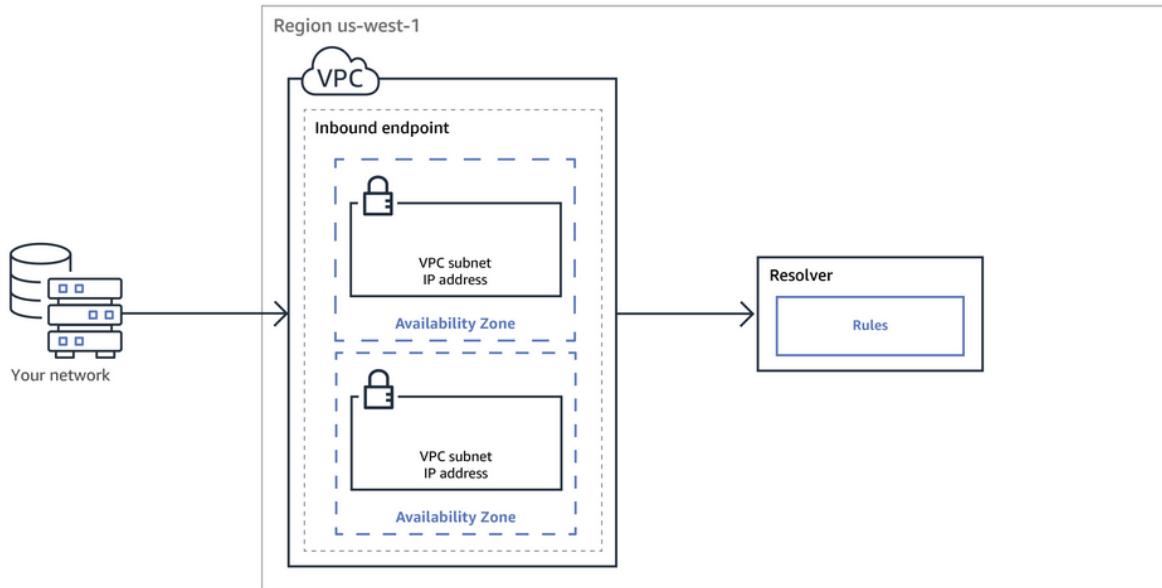
Like Amazon VPC, Resolver is regional. In each region where you have VPCs, you can choose whether to forward queries from your VPCs to your network (outbound queries), from your network to your VPCs (inbound queries), or both.

Note

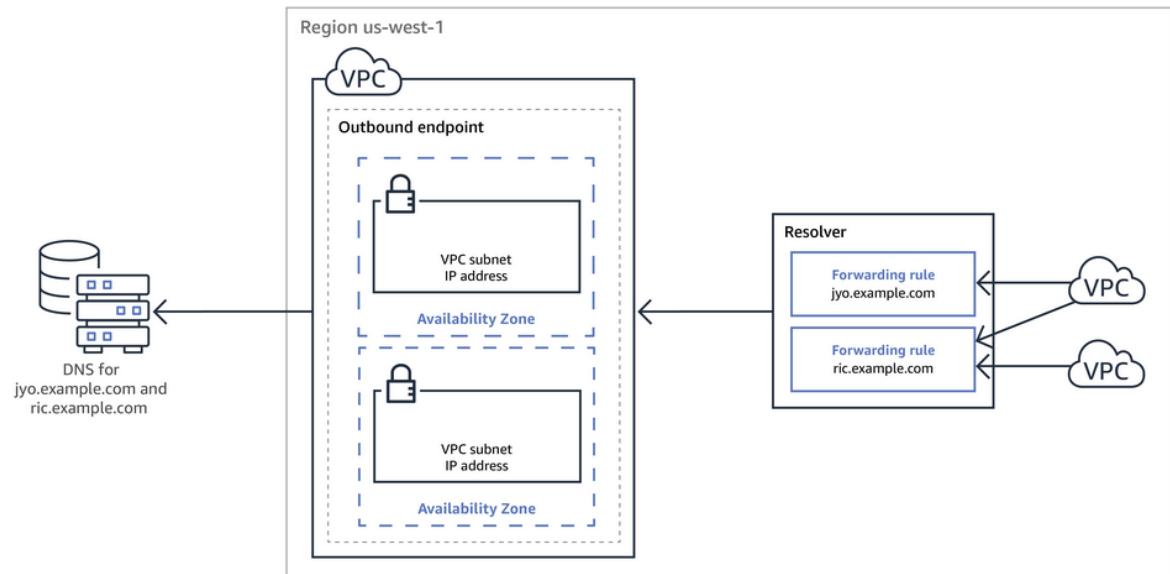
When you create a Resolver endpoint, you can't specify a VPC that has the instance tenancy attribute set to dedicated. For more information, see [Using Resolver in VPCs that are configured for dedicated instance tenancy](#).

To use inbound or outbound forwarding, you create a Resolver endpoint in your VPC. As part of the definition of an endpoint, you specify the IP addresses that you want to forward inbound DNS queries to or the IP addresses that you want outbound queries to originate from. For each IP address that you specify, Resolver automatically creates a VPC elastic network interface.

The following diagram shows the path of a DNS query from a DNS resolver on your network to Route 53 Resolver endpoints.



The following diagram shows the path of a DNS query from an EC2 instance in one of your VPCs to a DNS resolver on your network.



For an overview of VPC network interfaces, see [Elastic network interfaces](#) in the *Amazon VPC User Guide*.

Topics

- [How DNS resolvers on your network forward DNS queries to Route 53 Resolver endpoints \(p. 473\)](#)
- [How Route 53 Resolver endpoint forwards DNS queries from your VPCs to your network \(p. 473\)](#)
- [Considerations when creating inbound and outbound endpoints \(p. 478\)](#)

How DNS resolvers on your network forward DNS queries to Route 53 Resolver endpoints

When you want to forward DNS queries from your network to Route 53 Resolver endpoints in an AWS Region, you perform the following steps:

1. You create a Route 53 Resolver inbound endpoint in a VPC and specify the IP addresses that the resolvers on your network forward DNS queries to.

For each IP address that you specify for the inbound endpoint, Resolver creates a VPC elastic network interface in the VPC where you created the inbound endpoint.
2. You configure resolvers on your network to forward DNS queries for the applicable domain names to the IP addresses that you specified in the inbound endpoint. For more information, see [Considerations when creating inbound and outbound endpoints \(p. 478\)](#).

Here's how Resolver resolves DNS queries that originate on your network:

1. A web browser or another application on your network submits a DNS query for a domain name that you forwarded to Resolver.
2. A resolver on your network forwards the query to the IP addresses in your inbound endpoint.
3. The inbound endpoint forwards the query to Resolver.
4. Resolver gets the applicable value for the domain name in the DNS query, either internally or by performing a recursive lookup against public name servers.
5. Resolver returns the value (typically an IPv4 IP address) to the inbound endpoint.
6. The inbound endpoint returns the value to the resolver on your network.
7. The resolver on your network returns the value to the application.
8. Using the value that was returned by Resolver, the application submits an HTTP request, for example, a request for an object in an Amazon S3 bucket.

Creating an inbound endpoint doesn't change the behavior of Resolver, it just provides a path from a location outside the AWS network to Resolver.

How Route 53 Resolver endpoint forwards DNS queries from your VPCs to your network

When you want to forward DNS queries from the EC2 instances in one or more VPCs in an AWS Region to your network, you perform the following steps.

1. You create a Route 53 Resolver outbound endpoint in a VPC, and you specify several values:
 - The VPC that you want DNS queries to pass through on the way to the resolvers on your network.

- The IP addresses in your VPC that you want Resolver to forward DNS queries from. To hosts on your network, these are the IP addresses that the DNS queries originate from.
- A [VPC security group](#)

For each IP address that you specify for the outbound endpoint, Resolver creates an Amazon VPC elastic network interface in the VPC that you specify. For more information, see [Considerations when creating inbound and outbound endpoints \(p. 478\)](#).

2. You create one or more rules, which specify the domain names of the DNS queries that you want Resolver to forward to resolvers on your network. You also specify the IP addresses of the resolvers. For more information, see [Using rules to control which queries are forwarded to your network \(p. 474\)](#).
3. You associate each rule with the VPCs for which you want to forward DNS queries to your network.

Topics

- [Using rules to control which queries are forwarded to your network \(p. 474\)](#)
- [How Resolver determines whether the domain name in a query matches any rules \(p. 476\)](#)
- [How Resolver determines where to forward DNS queries \(p. 476\)](#)
- [Using rules in multiple Regions \(p. 477\)](#)
- [Domain names that Resolver creates autodefined system rules for \(p. 477\)](#)

Using rules to control which queries are forwarded to your network

Rules control which DNS queries Route 53 Resolver endpoint forwards to DNS resolvers on your network and which queries Resolver answers itself.

You can categorize rules in a couple of ways. One way is by who creates the rules:

- **Autodefined rules** – Resolver automatically creates autodefined rules and associates the rules with your VPCs. Most of these rules apply to the AWS-specific domain names that Resolver answers queries for. For more information, see [Domain names that Resolver creates autodefined system rules for \(p. 477\)](#).
- **Custom rules** – You create custom rules and associate the rules with VPCs. Currently, you can create only one type of custom rule, conditional forwarding rules, also known as forwarding rules. Forwarding rules cause Resolver to forward DNS queries from your VPCs to the IP addresses for DNS resolvers on your network.

If you create a forwarding rule for the same domain as an autodefined rule, Resolver forwards queries for that domain name to DNS resolvers on your network based on the settings in the forwarding rule.

Another way to categorize rules is by what they do:

- **Conditional forwarding rules** – You create conditional forwarding rules (also known as forwarding rules) when you want to forward DNS queries for specified domain names to DNS resolvers on your network.
- **System rules** – System rules cause Resolver to selectively override the behavior that is defined in a forwarding rule. When you create a system rule, Resolver resolves DNS queries for specified subdomains that would otherwise be resolved by DNS resolvers on your network.

By default, forwarding rules apply to a domain name and all its subdomains. If you want to forward queries for a domain to a resolver on your network but you don't want to forward queries for some

subdomains, you create a system rule for the subdomains. For example, if you create a forwarding rule for example.com but you don't want to forward queries for acme.example.com, you create a system rule and specify acme.example.com for the domain name.

- **Recursive rule** – Resolver automatically creates a recursive rule named **Internet Resolver**. This rule causes Route 53 Resolver to act as a recursive resolver for any domain names that you didn't create custom rules for and that Resolver didn't create autodefined rules for. For information about how to override this behavior, see "Forwarding All Queries to Your Network" later in this topic.

You can create custom rules that apply to specific domain names (yours or most AWS domain names), to public AWS domains names, or to all domain names.

Forwarding queries for specific domain names to your network

To forward queries for a specific domain name, such as example.com, to your network, you create a rule and specify that domain name. You also specify the IP addresses of the DNS resolvers on your network that you want to forward the queries to. You then associate each rule with the VPCs for which you want to forward DNS queries to your network. For example, you can create separate rules for example.com, example.org, and example.net. Then you can associate the rules with the VPCs in an AWS Region in any combination.

Forwarding queries for amazonaws.com to your network

The domain name amazonaws.com is the public domain name for AWS resources such as EC2 instances and S3 buckets. If you want to forward queries for amazonaws.com to your network, create a rule, specify amazonaws.com for the domain name, and specify **Forward** for the rule type.

Note

Resolver doesn't automatically forward DNS queries for some amazonaws.com subdomains even if you create a forwarding rule for amazonaws.com. For more information, see [Domain names that Resolver creates autodefined system rules for \(p. 477\)](#). For information about how to override this behavior, see "Forwarding All Queries to Your Network," immediately following.

Forwarding all queries to your network

If you want to forward all queries to your network, you create a rule, specify "." (dot) for the domain name, and associate the rule with the VPCs for which you want to forward all DNS queries to your network. Resolver still doesn't forward all DNS queries to your network because using a DNS resolver outside of AWS would break some functionality. For example, some internal AWS domain names have internal IP address ranges that aren't accessible from outside of AWS. For a list of the domain names for which queries aren't forwarded to your network when you create a rule for ".", see [Domain names that Resolver creates autodefined system rules for \(p. 477\)](#).

However, autodefined system rules for reverse DNS can be disabled, allowing the "." rule to forward all reverse DNS queries to your network. For more information on how to turn off the autodefined rules, see [Forwarding rules for reverse DNS queries in Resolver \(p. 495\)](#).

If you want to try forwarding DNS queries for all domain names to your network, including the domain names that are excluded from forwarding by default, you can create a "." rule and do one of the following:

- Set the `enableDnsHostnames` flag for the VPC to `false`
- Create rules for the domain names that are listed in [Domain names that Resolver creates autodefined system rules for \(p. 477\)](#)

Important

If you forward all domain names to your network, including the domain names that Resolver excludes when you create a "." rule, some features might stop working.

How Resolver determines whether the domain name in a query matches any rules

Route 53 Resolver compares the domain name in the DNS query with the domain name in the rules that are associated with the VPC that the query originated from. Resolver considers the domain names to match in the following cases:

- The domain names match exactly
- The domain name in the query is a subdomain of the domain name in the rule

For example, if the domain name in the rule is acme.example.com, Resolver considers the following domain names in a DNS query to be a match:

- acme.example.com
- zenith.acme.example.com

The following domain names are not a match:

- example.com
- nadir.example.com

If the domain name in a query matches the domain name in more than one rule (such as example.com and www.example.com), Resolver routes outbound DNS queries using the rule that contains the most specific domain name (www.example.com).

How Resolver determines where to forward DNS queries

When an application that runs on an EC2 instance in a VPC submits a DNS query, Route 53 Resolver performs the following steps:

1. Resolver checks for domain names in rules.

If the domain name in a query matches the domain name in a rule, Resolver forwards the query to the IP address that you specified when you created the outbound endpoint. The outbound endpoint then forwards the query to the IP addresses of resolvers on your network, which you specified when you created the rule.

For more information, see [How Resolver determines whether the domain name in a query matches any rules \(p. 476\)](#).

2. Resolver endpoint forwards DNS queries based on the settings in the "." rule.

If the domain name in a query doesn't match the domain name in any other rules, Resolver forwards the query based on the settings in the autodefined "." (dot) rule. The dot rule applies to all domain names except some AWS internal domain names and record names in private hosted zones. This rule causes Resolver to forward DNS queries to public name servers if the domain names in queries don't match any names in your custom forwarding rules. If you want to forward all queries to the DNS resolvers on your network, you can create a custom forwarding rule, specify "." for the domain name, specify **Forwarding** for **Type**, and specify the IP addresses of those resolvers.

3. Resolver returns the response to the application that submitted the query.

Using rules in multiple Regions

Route 53 Resolver is a regional service, so objects that you create in one AWS Region are available only in that Region. To use the same rule in more than one Region, you must create the rule in each Region.

The AWS account that created a rule can share the rule with other AWS accounts. For more information, see [Sharing forwarding rules with other AWS accounts and using shared rules \(p. 492\)](#).

Domain names that Resolver creates autodefined system rules for

Resolver automatically creates autodefined system rules that define how queries for selected domains are resolved by default:

- For private hosted zones and for Amazon EC2-specific domain names (such as `compute.amazonaws.com` and `compute.internal`), autodefined rules ensure that your private hosted zones and EC2 instances continue to resolve if you create conditional forwarding rules for less specific domain names such as "." (dot) or "com".
- For publicly reserved domain names (such as `localhost` and `10.in-addr.arpa`), DNS best practices recommend that queries are answered locally instead of being forwarded to public name servers. See [RFC 6303, Locally Served DNS Zones](#).

Note

If you create a conditional forwarding rule for "." (dot) or "com", we recommend that you also create a system rule for `amazonaws.com`. (System rules cause Resolver to locally resolve DNS queries for specific domains and subdomains.) Creating this system rule improves performance, reduces the number of queries that are forwarded to your network, and reduces Resolver charges.

If you want to override an autodefined rule, you can create a conditional forwarding rule for the same domain name.

You can also disable the autodefined rules. For more information, see [Forwarding rules for reverse DNS queries in Resolver \(p. 495\)](#).

Resolver creates the following autodefined rules.

Rules for private hosted zones

For each private hosted zone that you associate with a VPC, Resolver creates a rule and associates it with the VPC. If you associate the private hosted zone with multiple VPCs, Resolver associates the rule with the same VPCs.

The rule has a type of **Forward**.

Rules for various AWS internal domain names

All rules for the internal domain names in this section have a type of **Forward**. Resolver forwards DNS queries for these domain names to the authoritative name servers for the VPC.

Note

Resolver creates most of these rules when you set the `enableDnsHostnames` flag for a VPC to `true`. Resolver creates the rules even if you aren't using Resolver endpoints.

Resolver creates the following autodefined rules and associates them with a VPC when you set the `enableDnsHostnames` flag for the VPC to `true`:

- `Region-name.compute.internal`, for example, `eu-west-1.compute.internal`. The `us-east-1` Region doesn't use this domain name.

- *Region-name.compute.amazon-domain-name*, for example, eu-west-1.compute.amazonaws.com or cn-north-1.compute.amazonaws.com.cn. The us-east-1 Region doesn't use this domain name.
- ec2.internal. Only the us-east-1 Region uses this domain name.
- compute-1.internal. Only the us-east-1 Region uses this domain name.
- compute-1.amazonaws.com. Only the us-east-1 Region uses this domain name.

The following autodefined rules are for the reverse DNS lookup for the rules that Resolver creates when you set the `enableDnsHostnames` flag for the VPC to `true`.

- 10.in-addr.arpa
- 16.172.in-addr.arpa through 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Rules for each of the CIDR ranges for the VPC. For example, if a VPC that has a CIDR range of 10.0.0.0/23, Resolver creates the following rules:
 - 0.0.10.in-addr.arpa
 - 1.0.10.in-addr.arpa

The following autodefined rules, for localhost-related domains, also are created and associated with a VPC when you set the `enableDnsHostnames` flag for the VPC to `true`:

- localhost
- localdomain
- 127.in-addr.arpa
- 1.0.ip6.arpa
- 0.ip6.arpa

Resolver creates the following autodefined rules and associates them with your VPC when you connect the VPC with another VPC through transit gateway or VPC peering, and with DNS support enabled:

- The reverse DNS lookup for the peer VPC's IP address ranges, for example, 0.192.in-addr.arpa

If you add an IPv4 CIDR block to a VPC, Resolver adds an autodefined rule for the new IP address range.

- If the other VPC is in another Region, the following domain names:
 - *Region-name.compute.internal*. The us-east-1 Region doesn't use this domain name.
 - *Region-name.compute.amazon-domain-name*. The us-east-1 Region doesn't use this domain name.
 - ec2.internal. Only the us-east-1 Region uses this domain name.
 - compute-1.amazonaws.com. Only the us-east-1 Region uses this domain name.

A rule for all other domains

Resolver creates a "." (dot) rule that applies to all domain names that aren't specified earlier in this topic. The "." rule has a type of **Recursive**, which means that the rule causes Resolver to act as a recursive resolver.

Considerations when creating inbound and outbound endpoints

Before you create inbound and outbound Resolver endpoints in an AWS Region, consider the following issues.

Topics

- [Number of inbound and outbound endpoints in each Region](#)
- [Using the same VPC for inbound and outbound endpoints](#)
- [Inbound endpoints and private hosted zones](#)
- [VPC peering](#)
- [IP addresses in shared subnets](#)
- [Connection between your network and the VPCs that you create endpoints in](#)
- [When you share rules, you also share outbound endpoints](#)
- [Using Resolver in VPCs that are configured for dedicated instance tenancy](#)

Number of inbound and outbound endpoints in each AWS Region

When you want to integrate DNS for the VPCs in an AWS Region with DNS for your network, you typically need one Resolver inbound endpoint (for DNS queries that you're forwarding to your VPCs) and one outbound endpoint (for queries that you're forwarding from your VPCs to your network). You can create multiple inbound endpoints and multiple outbound endpoints, but one inbound or outbound endpoint is sufficient to handle the DNS queries for each respective direction. Note the following:

- For each Resolver endpoint, you specify two or more IP addresses in different Availability Zones. Each IP address in an endpoint can handle a large number of DNS queries per second. (For the current maximum number of queries per second per IP address in an endpoint, see [Quotas on Route 53 Resolver \(p. 673\)](#).) If you need Resolver to handle more queries, you can add more IP addresses to your existing endpoint instead of adding another endpoint.
- Resolver pricing is based on the number of IP addresses in your endpoints and on the number of DNS queries that the endpoint processes. Each endpoint includes a minimum of two IP addresses. For more information about Resolver pricing, see [Amazon Route 53 Pricing](#).
- Each rule specifies the outbound endpoint that DNS queries are forwarded from. If you create multiple outbound endpoints in an AWS Region and you want to associate some or all Resolver rules with every VPC, you need to create multiple copies of those rules.

Using the same VPC for inbound and outbound endpoints

You can create inbound and outbound endpoints in the same VPC or in different VPCs in the same Region.

For more information, see [Best practices for Amazon Route 53 \(p. 667\)](#).

Inbound endpoints and private hosted zones

If you want Resolver to resolve inbound DNS queries using records in a private hosted zone, associate the private hosted zone with the VPC that you created the inbound endpoint in. For information about associating private hosted zones with VPCs, see [Working with private hosted zones \(p. 356\)](#).

VPC peering

You can use any VPC in an AWS Region for an inbound or an outbound endpoint regardless of whether the VPC that you choose is peered with other VPCs. For more information, see [Amazon Virtual Private Cloud VPC peering](#).

IP addresses in shared subnets

When you create an inbound or outbound endpoint, you can specify an IP address in a shared subnet only if the current account created the VPC. If another account creates a VPC and shares a subnet in the VPC with your account, you can't specify an IP address in that subnet. For more information about shared subnets, see [Working with shared VPCs](#) in the *Amazon VPC User Guide*.

Connection between your network and the VPCs that you create endpoints in

You must have one of the following connections between your network and the VPCs that you create endpoints in:

- **Inbound endpoints** – You must set up either an [AWS Direct Connect](#) connection or a [VPN connection](#) between your network and each VPC that you create an inbound endpoint for.
- **Outbound endpoints** – You must set up an [AWS Direct Connect](#) connection, a [VPN connection](#), or a [network address translation \(NAT\) gateway](#) between your network and each VPC that you create an outbound endpoint for.

When you share rules, you also share outbound endpoints

When you create a rule, you specify the outbound endpoint that you want Resolver to use to forward DNS queries to your network. If you share the rule with another AWS account, you also indirectly share the outbound endpoint that you specify in the rule. If you used more than one AWS account to create VPCs in an AWS Region, you can do the following:

- Create one outbound endpoint in the Region.
- Create rules using one AWS account.
- Share the rules with all the AWS accounts that created VPCs in the Region.

This allows you to use one outbound endpoint in a Region to forward DNS queries to your network from multiple VPCs even if the VPCs were created using different AWS accounts.

Using Resolver in VPCs that are configured for dedicated instance tenancy

When you create a Resolver endpoint, you can't specify a VPC that has the [instance tenancy attribute](#) set to dedicated. Resolver doesn't run on single-tenant hardware.

You can still use Resolver to resolve DNS queries that originate in a VPC. Create at least one VPC that has the instance tenancy attribute set to default, and specify that VPC when you create inbound and outbound endpoints.

When you create a forwarding rule, you can associate it with any VPC, regardless of the setting for the instance tenancy attribute.

Getting started with Route 53 Resolver

The Route 53 Resolver console includes a wizard that guides you through the following steps for getting started with Resolver:

- Create endpoints: inbound, outbound, or both.
- For outbound endpoints, create one or more forwarding rules, which specify the domain names for which you want to route DNS queries to your network.
- If you created an outbound endpoint, choose the VPC that you want to associate the rules with.

To configure Route 53 Resolver using the wizard

1. Sign in to the AWS Management Console and open the Resolver console at <https://console.aws.amazon.com/route53resolver/>.
2. On the **Welcome to Route 53 Resolver** page, choose **Configure endpoints**.
3. On the navigation bar, choose the Region where you want to create a Resolver endpoint.
4. Under **Basic configuration**, choose the direction that you want to forward DNS queries:
 - **Inbound and outbound:** The wizard guides you through settings that let you both forward DNS queries from resolvers on your network to Resolver in a VPC, and forward specified queries (such as example.com or example.net) from a VPC to resolvers on your network.

- **Inbound only:** The wizard guides you through settings that let you forward DNS queries from resolvers on your network to Resolver in a VPC.
 - **Outbound only:** The wizard guides you through settings that let you forward specified queries from a VPC to resolvers on your network.
5. Choose **Next**.
 6. If you chose **Inbound and outbound** or **Inbound only**, enter the applicable values for configuring an inbound endpoint. Then continue with step 7. For more information, see [Values that you specify when you create or edit inbound endpoints \(p. 482\)](#).
If you choose **Outbound only**, skip to step 7.
 7. Enter the applicable values for configuring an outbound endpoint. For more information, see [Values that you specify when you create or edit outbound endpoints \(p. 484\)](#).
 8. If you chose **Inbound and outbound** or **Outbound only**, enter the applicable values for creating a rule. For more information, see [Values that you specify when you create or edit rules \(p. 485\)](#).
 9. On the **Review and create** page, confirm that the settings that you specified on previous pages are correct. If necessary, choose **Edit** for the applicable section, and update settings. When you're satisfied with the settings, choose **Submit**.
- Note**
Creating an outbound endpoint takes a minute or two. You can't create another outbound endpoint until the first one is created.
10. If you want to create more rules, see [Managing forwarding rules \(p. 490\)](#).
 11. If you created an inbound endpoint, configure DNS resolvers on your network to forward the applicable DNS queries to the IP addresses for your inbound endpoint. For more information, refer to the documentation for your DNS application.

Forwarding inbound DNS queries to your VPCs

To forward DNS queries from your network to Resolver, you create an inbound endpoint. An inbound endpoint specifies the IP addresses (from the range of IP addresses available to your VPC) that you want DNS resolvers on your network to forward DNS queries to. Those IP addresses aren't public IP addresses, so for each inbound endpoint, you need to connect your VPC to your network using either an AWS Direct Connect connection or a VPN connection.

Topics

- [Configuring inbound forwarding \(p. 481\)](#)
- [Values that you specify when you create or edit inbound endpoints \(p. 482\)](#)

Configuring inbound forwarding

To create an inbound endpoint, perform the following procedure.

To create an inbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Inbound endpoints**.
3. On the navigation bar, choose the Region where you want to create an inbound endpoint.
4. Choose **Create inbound endpoint**.
5. Enter the applicable values. For more information, see [Values that you specify when you create or edit inbound endpoints \(p. 482\)](#).

6. Choose **Create**.
7. Configure DNS resolvers on your network to forward the applicable DNS queries to the IP addresses for your inbound endpoint. For more information, refer to the documentation for your DNS application.

Values that you specify when you create or edit inbound endpoints

When you create or edit an inbound endpoint, you specify the following values:

Endpoint name

A friendly name that lets you easily find an inbound endpoint on the dashboard.

VPC in the *region-name* Region

All inbound DNS queries from your network pass through this VPC on the way to Resolver.

Security group for this endpoint

The ID of one or more security groups that you want to use to control access to this VPC. The security group that you specify must include one or more inbound rules. Inbound rules must allow TCP and UDP access on port 53.

For more information, see [Security groups for your VPC](#) in the *Amazon VPC User Guide*.

IP addresses

The IP addresses that you want DNS resolvers on your network to forward DNS queries to. We require you to specify a minimum of two IP addresses for redundancy. Note the following:

Multiple Availability Zones

We recommend that you specify IP addresses in at least two Availability Zones. You can optionally specify additional IP addresses in those or other Availability Zones.

IP addresses and Amazon VPC elastic network interfaces

For each combination of Availability Zone, Subnet, and IP address that you specify, Resolver creates an Amazon VPC elastic network interface. For the current maximum number of DNS queries per second per IP address in an endpoint, see [Quotas on Route 53 Resolver \(p. 673\)](#). For information about pricing for each elastic network interface, see "Amazon Route 53" on the [Amazon Route 53 pricing page](#).

For each IP address, specify the following values. Each IP address must be in an Availability Zone in the VPC that you specified in **VPC in the *region-name* Region**.

Availability Zone

The Availability Zone that you want DNS queries to pass through on the way to your VPC. The Availability Zone that you specify must be configured with a subnet.

Subnet

The subnet that contains the IP address that you want to forward DNS queries to. The subnet must have an available IP address.

Specify the subnet for an IPv4 address. IPv6 is not supported.

IP address

The IP address that you want to forward DNS queries to.

Choose whether you want Resolver to choose an IP address for you from among the available IP addresses in the specified subnet, or you want to specify the IP address yourself.

If you choose to specify the IP address yourself, enter an IPv4 address. IPv6 is not supported.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill; you can use also tags for other purposes. For more information about using tags for cost allocation, see [Using cost allocation tags in the AWS Billing and Cost Management User Guide](#).

Forwarding outbound DNS queries to your network

To forward DNS queries that originate on Amazon EC2 instances in one or more VPCs to your network, you create an outbound endpoint and one or more rules:

Outbound endpoint

To forward DNS queries from your VPCs to your network, you create an outbound endpoint. An outbound endpoint specifies the IP addresses that queries originate from. Those IP addresses, which you choose from the range of IP addresses available to your VPC, aren't public IP addresses. This means that, for each outbound endpoint, you need to connect your VPC to your network using AWS Direct Connect connection, a VPN connection, or a network address translation (NAT) gateway. Note that you can use the same outbound endpoint for multiple VPCs in the same Region, or you can create multiple outbound endpoints. If you want your outbound endpoint to use DNS64, you can enable DNS64 using Amazon Virtual Private Cloud. For more information, see [DNS64 and NAT64](#) in the *Amazon VPC User Guide*.

Rules

To specify the domain names of the queries that you want to forward to DNS resolvers on your network, you create one or more rules. Each rule specifies one domain name. You then associate rules with the VPCs for which you want to forward queries to your network.

For more information, see the following topics:

- [Private hosted zones that have overlapping namespaces](#)
- [Private hosted zones and Route 53 Resolver rules](#)

Configuring outbound forwarding

To configure Resolver to forward DNS queries that originate in your VPC to your network, perform the following procedures.

Important

After you create an outbound endpoint, you must create one or more rules and associate them with one or more VPCs. Rules specify the domain names of the DNS queries that you want to forward to your network.

To create an outbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

2. In the navigation pane, choose **Outbound endpoints**.
3. On the navigation bar, choose the Region where you want to create an outbound endpoint.
4. Choose **Create outbound endpoint**.
5. Enter the applicable values. For more information, see [Values that you specify when you create or edit outbound endpoints \(p. 484\)](#).
6. Choose **Create**.

Note

Creating an outbound endpoint takes a minute or two. You can't create another outbound endpoint until the first one is created.

7. Create one or more rules to specify the domain names of the DNS queries that you want to forward to your network. For more information, see the next procedure.

To create one or more forwarding rules, perform the following procedure.

To create forwarding rules and associate the rules with one or more VPCs

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you want to create the rule.
4. Choose **Create rule**.
5. Enter the applicable values. For more information, see [Values that you specify when you create or edit rules \(p. 485\)](#).
6. Choose **Save**.
7. To add another rule, repeat steps 4 through 6.

Values that you specify when you create or edit outbound endpoints

When you create or edit an outbound endpoint, you specify the following values:

Endpoint name

A friendly name that lets you easily find an outbound endpoint on the dashboard.

VPC in the *region-name* Region

All outbound DNS queries will flow through this VPC on the way to your network.

Security group for this endpoint

The ID of one or more security groups that you want to use to control access to this VPC. The security group that you specify must include an inbound rule for DNS (UDP) and DNS (TCP) from the Amazon Provided DNS for that VPC (VPC CIDR + 2). Outbound rules must allow TCP and UDP access on the port that you're using for DNS queries on your network. You can't change this value after you create an endpoint.

For more information, see [Security groups for your VPC](#) in the *Amazon VPC User Guide*.

IP addresses

The IP addresses in your VPC that you want Resolver to forward DNS queries to on the way to resolvers on your network. These are not the IP addresses of the DNS resolvers on your network; you

specify resolver IP addresses when you create the rules that you associate with one or more VPCs. We require you to specify a minimum of two IP addresses for redundancy.

Note the following:

Multiple Availability Zones

We recommend that you specify IP addresses in at least two Availability Zones. You can optionally specify additional IP addresses in those or other Availability Zones.

IP addresses and Amazon VPC elastic network interfaces

For each combination of Availability Zone, Subnet, and IP address that you specify, Resolver creates an Amazon VPC elastic network interface. For the current maximum number of DNS queries per second per IP address in an endpoint, see [Quotas on Route 53 Resolver \(p. 673\)](#). For information about pricing for each elastic network interface, see "Amazon Route 53" on the [Amazon Route 53 pricing page](#).

Order of IP addresses

You can specify IP addresses in any order. When forwarding DNS queries, Resolver doesn't choose IP addresses based on the order that the IP addresses are listed in.

For each IP address, specify the following values. Each IP address must be in an Availability Zone in the VPC that you specified in **VPC in the *region-name* Region**.

Availability Zone

The Availability Zone that you want DNS queries to pass through on the way to your network.
The Availability Zone that you specify must be configured with a subnet.

Subnet

The subnet that contains the IP address that you want DNS queries to originate from on the way to your network. The subnet must have an available IP address.

Specify the subnet for an IPv4 address. IPv6 is not supported.

IP address

The IP address that you want DNS queries to originate from on the way to your network.

Choose whether you want Resolver to choose an IP address for you from among the available IP addresses in the specified subnet, or you want to specify the IP address yourself.

If you choose to specify the IP address yourself, enter an IPv4 address. IPv6 is not supported.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill. For more information about using tags for cost allocation, see [Using cost allocation tags in the AWS Billing and Cost Management User Guide](#).

Values that you specify when you create or edit rules

When you create or edit a forwarding rule, you specify the following values:

Rule name

A friendly name that lets you easily find a rule on the dashboard.

Rule type

Choose the applicable value:

- **Forward** – Choose this option when you want to forward DNS queries for a specified domain name to resolvers on your network.
- **System** – Choose this option when you want Resolver to selectively override the behavior that is defined in a forwarding rule. When you create a system rule, Resolver resolves DNS queries for specified subdomains that would otherwise be resolved by DNS resolvers on your network.

By default, forwarding rules apply to a domain name and all its subdomains. If you want to forward queries for a domain to a resolver on your network but you don't want to forward queries for some subdomains, you create a system rule for the subdomains. For example, if you create a forwarding rule for example.com but you don't want to forward queries for acme.example.com, you create a system rule and specify acme.example.com for the domain name.

VPCs that use this rule

The VPCs that use this rule to forward DNS queries for the specified domain name or names. You can apply a rule to as many VPCs as you want.

Domain name

DNS queries for this domain name are forwarded to the IP addresses that you specify in **Target IP addresses**. For more information, see [How Resolver determines whether the domain name in a query matches any rules \(p. 476\)](#).

Outbound endpoint

Resolver forwards DNS queries through the outbound endpoint that you specify here to the IP addresses that you specify in **Target IP addresses**.

Target IP addresses

When a DNS query matches the name that you specify in **Domain name**, the outbound endpoint forwards the query to the IP addresses that you specify here. These are typically the IP addresses for DNS resolvers on your network.

Target IP addresses is available only when the value of **Rule type** is **Forward**.

Specify IPv4 addresses. IPv6 is not supported.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill. For more information about using tags for cost allocation, see [Using cost allocation tags in the AWS Billing and Cost Management User Guide](#).

Managing inbound endpoints

To manage inbound endpoints, perform the applicable procedure.

Topics

- [Viewing and editing inbound endpoints \(p. 487\)](#)
- [Viewing the status for inbound endpoints \(p. 487\)](#)

- [Deleting inbound endpoints \(p. 488\)](#)

Viewing and editing inbound endpoints

To view and edit settings for an inbound endpoint, perform the following procedure.

To view and edit settings for an inbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 2. In the navigation pane, choose **Inbound endpoints**.
 3. On the navigation bar, choose the Region where you created the inbound endpoint.
 4. Choose the option for the endpoint that you want to view settings for or want to edit.
 5. Choose **View details** or **Edit**.
- For information about the values for inbound endpoints, see [Values that you specify when you create or edit inbound endpoints \(p. 482\)](#).
6. If you chose **Edit**, enter the applicable values, and choose **Save**.

Viewing the status for inbound endpoints

To view the status for an inbound endpoint, perform the following procedure.

To view the status for an inbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Inbound endpoints**.
3. On the navigation bar, choose the Region where you created the inbound endpoint. The **Status** column contains one of the following values:

Creating

Resolver is creating and configuring one or more Amazon VPC network interfaces for this endpoint.

Operational

The Amazon VPC network interfaces for this endpoint are correctly configured and able to pass inbound or outbound DNS queries between your network and Resolver.

Updating

Resolver is associating or disassociating one or more network interfaces with this endpoint.

Auto recovering

Resolver is trying to recover one or more of the network interfaces that are associated with this endpoint. During the recovery process, the endpoint functions with limited capacity because of the limit on the number of DNS queries per IP address (per network interface). For the current limit, see [Quotas on Route 53 Resolver \(p. 673\)](#).

Action needed

This endpoint is unhealthy, and Resolver can't automatically recover it. To resolve the problem, we recommend that you check each IP address that you associated with the endpoint. For each IP address that isn't available, add another IP address and then delete the IP address that

isn't available. (An endpoint must always include at least two IP addresses.) A status of **Action needed** can have a variety of causes. Here are two common causes:

- One or more of the network interfaces that are associated with the endpoint were deleted using Amazon VPC.
- The network interface couldn't be created for some reason that's outside the control of Resolver.

Deleting

Resolver is deleting this endpoint and the associated network interfaces.

Deleting inbound endpoints

To delete an inbound endpoint, perform the following procedure.

Important

If you delete an inbound endpoint, DNS queries from your network are no longer forwarded to Resolver in the VPC that you specified in the endpoint.

To delete an inbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Inbound endpoints**.
3. On the navigation bar, choose the Region where you created the inbound endpoint.
4. Choose the option for the endpoint that you want to delete.
5. Choose **Delete**.
6. To confirm that you want to delete the endpoint, enter the name of the endpoint and choose **Submit**.

Managing outbound endpoints

To manage outbound endpoints, perform the applicable procedure.

Topics

- [Viewing and editing outbound endpoints \(p. 488\)](#)
- [Viewing the status for outbound endpoints \(p. 489\)](#)
- [Deleting outbound endpoints \(p. 489\)](#)

Viewing and editing outbound endpoints

To view and edit settings for an outbound endpoint, perform the following procedure.

To view and edit settings for an outbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Outbound endpoints**.
3. On the navigation bar, choose the Region where you created the outbound endpoint.
4. Choose the option for the endpoint that you want to view settings for or want to edit.

5. Choose **View details or Edit**.

For information about the values for outbound endpoints, see [Values that you specify when you create or edit outbound endpoints \(p. 484\)](#).

6. If you chose **Edit**, enter the applicable values, and then choose **Save**.

Viewing the status for outbound endpoints

To view the status for an outbound endpoint, perform the following procedure.

To view the status for an outbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Outbound endpoints**.
3. On the navigation bar, choose the Region where you created the outbound endpoint. The **Status** column contains one of the following values:

Creating

Resolver is creating and configuring one or more Amazon VPC network interfaces for this endpoint.

Operational

The Amazon VPC network interfaces for this endpoint are correctly configured and able to pass inbound or outbound DNS queries between your network and Resolver.

Updating

Resolver is associating or disassociating one or more network interfaces with this endpoint.

Auto recovering

Resolver is trying to recover one or more of the network interfaces that are associated with this endpoint. During the recovery process, the endpoint functions with limited capacity because of the limit on the number of DNS queries per IP address (per network interface). For the current limit, see [Quotas on Route 53 Resolver \(p. 673\)](#).

Action needed

This endpoint is unhealthy, and Resolver can't automatically recover it. To resolve the problem, we recommend that you check each IP address that you associated with the endpoint. For each IP address that isn't available, add another IP address and then delete the IP address that isn't available. (An endpoint must always include at least two IP addresses.) A status of **Action needed** can have a variety of causes. Here are two common causes:

- One or more of the network interfaces that are associated with the endpoint were deleted using Amazon VPC.
- The network interface couldn't be created for some reason that's outside the control of Resolver.

Deleting

Resolver is deleting this endpoint and the associated network interfaces.

Deleting outbound endpoints

To delete an outbound endpoint, perform the following procedure.

Important

If you delete an outbound endpoint, Resolver stops forwarding DNS queries from your VPC to your network for rules that specify the deleted outbound endpoint.

To delete an outbound endpoint

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Outbound endpoints**.
3. On the navigation bar, choose the Region where you created the outbound endpoint.
4. Choose the option for the endpoint that you want to delete.
5. Choose **Delete**.
6. To confirm that you want to delete the endpoint, enter the name of the endpoint, and then choose **Submit**.

Managing forwarding rules

If you want Resolver to forward queries for specified domain names to your network, you create one forwarding rule for each domain name and specify the name of the domain for which you want to forward queries.

Topics

- [Viewing and editing forwarding rules \(p. 490\)](#)
- [Creating forwarding rules \(p. 491\)](#)
- [Adding rules for reverse lookup \(p. 491\)](#)
- [Associating forwarding rules with a VPC \(p. 491\)](#)
- [Disassociating forwarding rules from a VPC \(p. 492\)](#)
- [Sharing forwarding rules with other AWS accounts and using shared rules \(p. 492\)](#)
- [Deleting forwarding rules \(p. 494\)](#)
- [Forwarding rules for reverse DNS queries in Resolver \(p. 495\)](#)

Viewing and editing forwarding rules

To view and edit settings for a forwarding rule, perform the following procedure.

To view and edit settings for a forwarding rule

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you created the rule.
4. Choose the option for the rule that you want to view settings for or want to edit.
5. Choose **View details** or **Edit**.

For information about the values for forwarding rules, see [Values that you specify when you create or edit rules \(p. 485\)](#).
6. If you chose **Edit**, enter the applicable values, and then choose **Save**.

Creating forwarding rules

To create one or more forwarding rules, perform the following procedure.

To create forwarding rules and associate the rules with one or more VPCs

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you want to create the rule.
4. Choose **Create rule**.
5. Enter the applicable values. For more information, see [Values that you specify when you create or edit rules \(p. 485\)](#).
6. Choose **Save**.
7. To add another rule, repeat steps 4 through 6.

Adding rules for reverse lookup

If you need to control reverse lookups in your VPC, you can add rules to your outbound resolver endpoint.

To create the reverse lookup rule

1. Follow the steps in the previous procedure, up to step 5.
2. When you specify your rule, enter the PTR record for the IP address or addresses that you want a reverse lookup forwarding rule for.

For example, if you need to forward lookups for addresses in the 10.0.0.0/23 range, enter two rules:

- 0.0.10.in-addr.arpa
- 1.0.10.in-addr.arpa

Any IP address in those subnets will be referenced as a subdomain of those PTR records—for example, 10.0.1.161 will have a reverse lookup address of 161.1.0.10.in-addr.arpa, which is a subdomain of 1.0.10.in-addr.arpa.

3. Specify the server to forward these lookups to.
4. Add these rules to your outbound resolver endpoint.

Note that turning on `enableDNSHostNames` for your VPC automatically adds PTR records. See [Resolving DNS queries between VPCs and your network \(p. 471\)](#). The previous procedure is required only if you want to explicitly specify a resolver for given IP ranges—for example, when forwarding queries to an Active Directory server.

Associating forwarding rules with a VPC

After you create a forwarding rule, you must associate the rule with one or more VPCs. When you associate a rule with a VPC, Resolver starts to forward DNS queries for the domain name that's specified in the rule to the DNS resolvers that you specified in the rule. The queries pass through the outbound endpoint that you specified when you created the rule.

To associate a forwarding rule with one or more VPCs

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you created the rule.
4. Choose the name of the rule that you want to associate with one or more VPCs.
5. Choose **Associate VPC**.
6. Under **VPCs that use this rule**, choose the VPCs that you want to associate the rule with.
7. Choose **Add**.

Disassociating forwarding rules from a VPC

You disassociate a forwarding rule from a VPC in the following circumstances:

- For DNS queries that originate in this VPC, you want Resolver to stop forwarding queries for the domain name specified in the rule to your network.
- You want to delete the forwarding rule. If a rule is currently associated with one or more VPCs, you must disassociate the rule from all VPCs before you can delete it.

If you want to disassociate a forwarding rule from one or more VPCs, perform the following procedure.

To disassociate a forwarding rule from a VPC

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you created the rule.
4. Choose the name of the rule that you want to disassociate from one or more VPCs.
5. Choose the option for the VPC that you want to disassociate the rule from.
6. Choose **Disassociate**.
7. Type **disassociate** to confirm.
8. Choose **Submit**.

Sharing forwarding rules with other AWS accounts and using shared rules

You can share the forwarding rules that you created using one AWS account with other AWS accounts. To share rules, the Route 53 Resolver console integrates with AWS Resource Access Manager. For more information about Resource Access Manager, see the [Resource Access Manager User Guide](#).

Note the following:

Associating shared rules with VPCs

If another AWS account has shared one or more rules with your account, you can associate the rules with your VPCs the same way that you associate rules that you created with your VPCs. For more information, see [Associating forwarding rules with a VPC \(p. 491\)](#).

Deleting or unsharing a rule

If you share a rule with other accounts and then either delete the rule or stop sharing it, and if the rule was associated with one or more VPCs, Route 53 Resolver starts to process DNS queries for those VPCs based on the remaining rules. The behavior is the same as if you disassociate the rule from the VPC.

Maximum number of rules and associations

When an account creates a rule and shares it with one or more other accounts, the maximum number of rules per AWS Region applies to the account that created the rule.

When an account that a rule is shared with associates the rule with one or more VPCs, the maximum number of associations between rules and VPCs per Region applies to the account that the rule is shared with.

For current Resolver quotas, see [Quotas on Route 53 Resolver \(p. 673\)](#).

Permissions

To share a rule with another AWS account, you must have permission to use the [PutResolverRulePolicy](#) action.

Restrictions on the AWS account that a rule is shared with

The account that a rule is shared with can't change or delete the rule.

Tagging

Only the account that created a rule can add, delete, or see tags on the rule.

To view the current sharing status of a rule (including the account that shared the account or the account that a rule is shared with), and to share rules with another account, perform the following procedure.

To view sharing status and share rules with another AWS account

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you created the rule.

The **Sharing status** column shows the current sharing status of rules that were created by the current account or that are shared with the current account:

- **Not shared:** The current AWS account created the rule, and the rule is not shared with any other accounts.
 - **Shared by me:** The current account created the rule and shared it with one or more accounts.
 - **Shared with me:** Another account created the rule and shared it with the current account.
4. Choose the name of the rule that you want to display sharing information for or that you want to share with another account.

On the **Rule: rule name** page, the value under **Owner** displays ID of the account that created the rule. That's the current account unless the value of **Sharing status** is **Shared with me**. In that case, **Owner** is the account that created the rule and shared it with the current account.

5. Choose **Share** to view additional information or to share the rule with another account. A page in the Resource Access Manager console appears, depending on the value of **Sharing status**:
 - **Not shared:** The **Create resource share** page appears. For information about how to share the rule with another account, OU, or organization, skip to step 6.

- **Shared by me:** The **Shared resources** page shows the rules and other resources that are owned by the current account and shared with other accounts.
 - **Shared with me:** The **Shared resources** page shows the rules and other resources that are owned by other accounts and shared with the current account.
6. To share a rule with another AWS account, OU, or organization, specify the following values.

Note

You can't update sharing settings. If you want to change any of the following settings, you must reshare a rule with the new settings and then remove the old sharing settings.

Description

Enter a short description that helps you remember why you shared the rule.

Resources

Choose the check box for the rule that you want to share.

Principals

Enter the AWS account number, OU name, or organization name.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill; you can use also tags for other purposes. For more information about using tags for cost allocation, see [Using cost allocation tags](#) in the *AWS Billing and Cost Management User Guide*.

Deleting forwarding rules

To delete a forwarding rule, perform the following procedure.

Note the following:

- If the forwarding rule is associated with any VPCs, you must disassociate the rule from the VPCs before you can delete the rule. For more information, see [Disassociating forwarding rules from a VPC \(p. 492\)](#).
- You can't delete the default **Internet Resolver** rule, which has a value of **Recursive** for **Type**. This rule causes Route 53 Resolver to act as a recursive resolver for any domain names that you didn't create custom rules for and that Resolver didn't create autodefined rules for. For more information about how rules are categorized, see [Using rules to control which queries are forwarded to your network \(p. 474\)](#).

To delete a forwarding rule

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rules**.
3. On the navigation bar, choose the Region where you created the rule.
4. Choose the option for the rule that you want to delete.
5. Choose **Delete**.
6. To confirm that you want to delete the rule, enter the name of the rule and choose **Submit**.

Forwarding rules for reverse DNS queries in Resolver

When the `enableDnsHostnames` and `enableDnsSupport` are set to `true` for a virtual private cloud (VPC) from Amazon VPC, Resolver automatically creates auto-defined system rules for reverse DNS queries. For more information about these settings, see [DNS attributes in your VPC](#) in the *Amazon VPC Developer Guide*.

Forwarding rules for reverse DNS queries are particularly useful for services like SSH or Active Directory, which have an option to authenticate users by performing a reverse DNS lookup for the IP address from which a customer is attempting to connect to a resource. For more information about auto-defined system rules, see [Domain names that Resolver creates autodefined system rules for \(p. 477\)](#).

You can turn off these rules and modify all reverse DNS queries so that they are, for example, forwarded to your on-premises name servers for resolution.

After you turn off the automatic rules, create rules to forward the queries as needed to your on-premises resources. For more information about how to manage forwarding rules, see [Managing forwarding rules \(p. 490\)](#).

To turn off auto-defined rules

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, under **Resolver** choose **VPCs**, and then choose a VPC ID.
3. Under **Autodefined rules for reverse DNS resolution**, deselect the check box. If the check box is already deselected, you can select it to turn on auto-defined reverse DNS resolution.

For the related APIs, see [Resolver configuration APIs](#).

Enabling DNSSEC validation in Amazon Route 53

When you enable DNSSEC validation for a virtual private cloud (VPC) in Amazon Route 53, DNSSEC signatures are cryptographically checked to ensure that the response was not tampered with. You enable DNSSEC validation on your VPC detail page.

DNSSEC validation only applies to public signed names in Amazon Route 53, and not to forwarded zones.

Important

Enabling DNSSEC validation can impact DNS resolution for public DNS records from AWS resources in a VPC, which could result in an outage. Be aware that enabling or disabling DNSSEC validation can take several minutes.

To enable DNSSEC validation for a VPC

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, under **Resolver**, choose **VPCs**.
3. Under **DNSSEC validation**, select the checkbox. If the checkbox is already selected, you can clear it to disable DNSSEC validation.

Be aware that enabling or disabling DNSSEC validation can take several minutes.

Routing internet traffic to your AWS resources

You can use Amazon Route 53 to route traffic to a variety of AWS resources.

- Routing traffic to an Amazon API Gateway API by using your domain name (p. 496)
- Routing traffic to an Amazon CloudFront distribution by using your domain name (p. 498)
- Routing traffic to an Amazon EC2 instance (p. 500)
- Routing traffic to an AWS Elastic Beanstalk environment (p. 502)
- Routing traffic to an ELB load balancer (p. 505)
- Routing traffic to a website that is hosted in an Amazon S3 bucket (p. 507)
- Routing traffic to an Amazon Virtual Private Cloud interface endpoint by using your domain name (p. 509)
- Routing traffic to Amazon WorkMail (p. 511)
- Routing traffic to other AWS resources (p. 513)
- Creating Amazon Route 53 and Amazon Route 53 Resolver resources with AWS CloudFormation (p. 513)

Routing traffic to an Amazon API Gateway API by using your domain name

Amazon API Gateway lets you create, publish, maintain, monitor, and secure APIs. You can create APIs that access AWS services or other web services, as well as data stored in the AWS Cloud.

The method that you use to route domain traffic to an API Gateway API is the same regardless of whether you created a regional API Gateway endpoint or an edge-optimized API Gateway endpoint.

- **Regional API endpoint:** You create a Route 53 alias record that routes traffic to the regional API endpoint.
- **Edge-optimized API endpoint:** You create a Route 53 alias record that routes traffic to the edge-optimized API. This causes traffic to be routed to the CloudFront distribution that's associated with the edge-optimized API.

An alias record is a Route 53 extension to DNS that's similar to a CNAME record. For a comparison of alias and CNAME records, see [Choosing between alias and non-alias records \(p. 379\)](#).

Note

Route 53 doesn't charge for alias queries to API Gateway APIs or other AWS resources.

Topics

- [Prerequisites \(p. 496\)](#)
- [Configuring Route 53 to route traffic to an API Gateway endpoint \(p. 497\)](#)

Prerequisites

Before you get started, you need the following:

- An API Gateway API that has a custom domain name, such as `api.example.com`, that matches the name of the Route 53 record that you want to create.

For more information see:

- [Setting up custom domain names for HTTP APIs in the Amazon API Gateway Developer Guide](#).
- [Setting up custom domain names for REST APIs in the Amazon API Gateway Developer Guide](#).
- [Setting up custom domain names for WebSocket APIs in the Amazon API Gateway Developer Guide](#).
- A registered domain name. You can use Amazon Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

For information about using Route 53 as the DNS service provider for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Configuring Route 53 to route traffic to an API Gateway endpoint

To configure Route 53 to route traffic to an API Gateway endpoint, perform the following procedure.

To route traffic to an API Gateway endpoint

1. If you created the Route 53 hosted zone and the endpoint using the same account, skip to step 2.

If you created the hosted zone and the endpoint using different accounts, get the target domain name for the custom domain name that you want to use:

- a. Sign in to the AWS Management Console and open the API Gateway console at <https://console.aws.amazon.com/apigateway/>.
 - b. In the navigation pane, choose **Custom domain names**.
 - c. For the custom domain name that you want to use, get the value of **API Gateway domain name**.
2. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 3. In the navigation pane, choose **Hosted zones**.
 4. Choose the name of the hosted zone that has the domain name that you want to use to route traffic to your API.
 5. Choose **Create record**.
 6. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your API.

The API that you want to route traffic to must include a custom domain name, such as `api.example.com`, that matches the name of the Route 53 record.

Alias

If you are using the **Quick create** record creation method, turn on **Alias**.

API Version 2013-04-01

Value/Route traffic to

Choose **Alias to API Gateway API**, then choose the Region that the endpoint is from.

How you specify the value for **Endpoint** depends on whether you created the hosted zone and the API using the same AWS account or different accounts:

- **Same account** – The list of target domain names includes only APIs that have a custom domain name that matches the value that you specified for **Record name**. Choose the applicable value.
- **Different accounts** – Enter the value that you got in step 1 of this procedure.

Record type

Choose **A – IPv4 address**.

Evaluate target health

Accept the default value of **Yes**.

7. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your API by using the name of the alias record that you created in this procedure.

Routing traffic to an Amazon CloudFront distribution by using your domain name

If you want to speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website—including dynamic, static, streaming, and interactive content—by using a global network of edge locations. Requests for your content are automatically routed to the edge location that gives your users the lowest latency.

Note

You can route traffic to a CloudFront distribution only for public hosted zones.

To use CloudFront to distribute your content, you create a distribution and specify settings such as the Amazon S3 bucket or HTTP server that you want CloudFront to get your content from, whether you want only selected users to have access to your content, and whether you want to require users to use HTTPS.

When you create a distribution, CloudFront assigns a domain name to the distribution, such as d111111abcdef8.cloudfront.net. You can use this domain name in the URLs for your content, for example:

`http://d111111abcdef8.cloudfront.net/logo.jpg`

Alternatively, you might prefer to use your own domain name in URLs, for example:

`http://example.com/logo.jpg`

If you want to use your own domain name, use Amazon Route 53 to create an [alias record](#) that points to your CloudFront distribution. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as example.com, and for subdomains, such as www.example.com. (You can create CNAME records only for subdomains.) When Route 53 receives a DNS query that matches the name and type of an alias record, Route 53 responds with the domain name that is associated with your distribution.

Note

Route 53 doesn't charge for alias queries to CloudFront distributions or other AWS resources.

Prerequisites

Before you get started, you need the following:

- A CloudFront distribution. The distribution must include an alternate domain name that matches the domain name that you want to use for your URLs instead of the domain name that CloudFront assigned to your distribution.

For example, if you want the URLs for your content to contain the domain name **example.com**, the **Alternate Domain Name** field for the distribution must include **example.com**.

For more information, see the following documentation in the *Amazon CloudFront Developer Guide*:

- [Task list for creating a distribution](#)
- [Creating or updating a distribution using the CloudFront console](#)
- A registered domain name. You can use Amazon Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

For information about using Route 53 as the DNS service provider for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Configuring Amazon Route 53 to route traffic to a CloudFront distribution

To configure Amazon Route 53 to route traffic to a CloudFront distribution, perform the following procedure.

Note

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your CloudFront distribution by using the name of the alias record that you create in this procedure.

To route traffic to a CloudFront distribution

1. Get the domain name that CloudFront assigned to your distribution, and determine whether IPv6 is enabled:
 - a. Sign in to the AWS Management Console and open the CloudFront console at <https://console.aws.amazon.com/cloudfront/v3/home>.
 - b. in the **ID** column, select the linked name of the distribution that you want to route traffic to (not the check box).
 - c. On the **General** tab, get the value of the **Distribution domain name** field.
 - d. Check the **IPv6** field to see whether IPv6 is enabled for the distribution. If IPv6 is enabled, you'll need to create two alias records for the distribution, one to route IPv4 traffic to the distribution, and one to route IPv6 traffic.

For more information, see [Enable IPv6](#) in the topic [Values that you specify when you create or update a distribution](#) in the *Amazon CloudFront Developer Guide*.

2. If you haven't already, add one or more alternate domain names to your CloudFront distribution. These are the domain names (such as `example.com`) and subdomain names (such as `acme.example.com`) that you want to use for your URLs instead of the domain name that CloudFront assigned to your distribution.

For more information, see [Using custom URLs for files by adding alternate domain names \(CNAMEs\) in the Amazon CloudFront Developer Guide](#).

3. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
4. In the navigation pane, choose **Hosted zones**.
5. Choose the linked name of the hosted zone for the domain that you want to use to route traffic to your CloudFront distribution.
6. Choose **Create record**.

You can use the wizard to create the records, or choose **Switch to quick create**.

7. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your CloudFront distribution. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use **acme.example.com** to route traffic to your distribution, enter **acme**.

Alias

If you are using the **Quick create** record creation method, turn on **Alias**.

Important

You must create an Alias record for the CloudFront distribution to work.

Value/Route traffic to

Choose **Alias to CloudFront distributions**. The us-east-1 Region is selected by default. Choose the name that CloudFront assigned to the distribution when you created it. This is the value that you got in step 1.

Record type

Choose **A – IPv4 address**.

If IPv6 is enabled for the distribution and you're creating a second record, choose **AAAA – IPv6 address**.

Evaluate target health

Accept the default value of **No**.

8. Choose **Create records**.
9. If IPv6 is enabled for the distribution, repeat steps 6 through 8. Specify the same settings except for the **Record type** field, as explained in step 7.

Routing traffic to an Amazon EC2 instance

Amazon EC2 provides scalable computing capacity in the AWS cloud. You can launch an EC2 virtual computing environment (an instance) using a preconfigured template (an Amazon Machine Image, or AMI). When you launch an EC2 instance, EC2 automatically installs the operating system (Linux or Microsoft Windows) and additional software included in the AMI, such as web server or database software.

If you're hosting a website or running a web application on an EC2 instance, you can route traffic for your domain, such as example.com, to your server by using Amazon Route 53.

Prerequisites

Before you get started, you need the following:

- An Amazon EC2 instance. For information about launching an EC2 instance, see the following documentation:
 - **Linux** – See [Getting started with Amazon EC2 Linux instances](#) in the *Amazon EC2 User Guide for Linux Instances*
 - **Microsoft Windows** – See [Getting started with Amazon EC2 Windows instances](#) in the *Amazon EC2 User Guide for Windows Instances*

Important

We recommend that you also create an [Elastic IP address](#) and associate it with your EC2 instance. An Elastic IP address ensures that the IP address of your Amazon EC2 instance will never change. For information related to pricing, see [Pricing for Elastic IP addresses](#).

- A registered domain name. You can use Amazon Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

For information about using Route 53 as the DNS service provider for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Configuring Amazon Route 53 to route traffic to an Amazon EC2 instance

To configure Amazon Route 53 to route traffic to an EC2 instance, perform the following procedure.

To route traffic to an Amazon EC2 instance

1. Get the IP address for the Amazon EC2 instance:
 - a. Sign in to the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
 - b. In the Regions list in the upper right corner of the console, choose the Region that you launched the instance in.
 - c. In the navigation pane, choose **Instances**.
 - d. In the table, choose the instance that you want to route traffic to.
 - e. In the bottom pane, on the **Description** tab, get the value of **Elastic IPs**.

If you didn't associate an Elastic IP with the instance, get the value of **IPv4 Public IP**.
2. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Hosted zones**.
4. Choose the name of the hosted zone that matches the name of the domain that you want to route traffic for.
5. Choose **Create record**.
6. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your EC2 instance. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use acme.example.com to route traffic to your EC2 instance, enter **acme**.

Value/Route traffic to

Choose **IP address or another value depending on the record type**. Enter the IP address that you got in step 1.

Record type

Choose **A – IPv4 address**.

TTL (seconds)

Accept the default value of **300**.

7. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your EC2 instance by using the name of the record that you created in this procedure.

Routing traffic to an AWS Elastic Beanstalk environment

If you're using AWS Elastic Beanstalk to deploy and manage applications in the AWS Cloud, you can use Amazon Route 53 to route DNS traffic for your domain, such as example.com, to a new or an existing Elastic Beanstalk environment.

To route DNS traffic to an Elastic Beanstalk environment, see the procedures in the following topics.

Note

These procedures assume that you're already using Route 53 as the DNS service for your domain. If you're using another DNS service, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#) for information about using Route 53 as the DNS service provider for your domain.

Topics

- [Deploying an application into an Elastic Beanstalk environment \(p. 503\)](#)
- [Getting the domain name for your Elastic Beanstalk environment \(p. 503\)](#)
- [Creating an Amazon Route 53 record that routes traffic to your Elastic Beanstalk environment \(p. 503\)](#)

Deploying an application into an Elastic Beanstalk environment

If you already have an Elastic Beanstalk environment that you want to route traffic to, skip to [Getting the domain name for your Elastic Beanstalk environment \(p. 503\)](#).

To create an application and deploy it into an Elastic Beanstalk environment

- For information about creating an application and deploying it to an Elastic Beanstalk environment, see [Getting started using Elastic Beanstalk](#) in the *AWS Elastic Beanstalk Developer Guide*.

Getting the domain name for your Elastic Beanstalk environment

If you already know the domain name for your Elastic Beanstalk environment, skip to [Creating an Amazon Route 53 record that routes traffic to your Elastic Beanstalk environment \(p. 503\)](#).

To get the domain name for your Elastic Beanstalk environment

1. Sign in to the AWS Management Console and open the Elastic Beanstalk console at <https://console.aws.amazon.com/elasticbeanstalk/>.
2. In the list of applications, find the application that you want to route traffic to, and get the value of **URL**. If you don't see the list of applications, choose **Applications** in the navigation pane.

For more information about the URL, see [Elastic Beanstalk environment's domain name](#) in the *Elastic Beanstalk developer guide*.

Creating an Amazon Route 53 record that routes traffic to your Elastic Beanstalk environment

An Amazon Route 53 record contains the settings that control how traffic is routed to your Elastic Beanstalk environment. You create either a *CNAME record* or an *alias record*, depending on whether the domain name for the environment includes the Region, such as **us-east-2**, in which you deployed the environment. New environments include the Region in the domain name; environments that were created before early 2016 do not. For a comparison of CNAME and alias records, see [Choosing between alias and non-alias records \(p. 379\)](#).

If the domain name does not include the Region

You must create a *CNAME record*. However, because of limitations imposed by DNS, you can create CNAME records only for subdomains, not for the root domain name. For example, if your domain name is example.com, you can create a record that routes traffic for acme.example.com to your Elastic Beanstalk environment, but you can't create a record that routes traffic for example.com to your Elastic Beanstalk environment.

See the procedure [To create a CNAME record to route traffic to an Elastic Beanstalk environment \(p. 504\)](#).

If the domain name includes the Region

You can create an alias record. An alias record is specific to Route 53 and has two significant advantages over CNAME records:

- You can create alias records for the root domain name or for subdomains. For example, if your domain name is example.com, you can create a record that routes requests for example.com or for acme.example.com to your Elastic Beanstalk environment.
- Route 53 doesn't charge for requests that use an alias record to route traffic.

See the procedure [To create an Amazon Route 53 alias record to route traffic to an Elastic Beanstalk environment \(p. 505\)](#).

To create a CNAME record to route traffic to an Elastic Beanstalk environment

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Choose the name of the hosted zone that you want to use to route traffic to your Elastic Beanstalk environment.
4. Choose **Create record**.
5. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your Elastic Beanstalk environment. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use acme.example.com to route traffic to your environment, enter **acme**.

Important

You can't create a CNAME record that has the same name as the hosted zone.

Alias

If you are using the **Quick create** record creation method, turn on **Alias**.

Value/Route traffic to

Choose **IP address or another value depending on the record type** and enter the value that you get when you perform the procedure in the topic [Getting the domain name for your Elastic Beanstalk environment \(p. 503\)](#). If you used different accounts to create your Route 53 hosted zone and your Elastic Beanstalk environment, enter the CNAME attributes for the Elastic Beanstalk environment.

Record type

Choose **CNAME**.

TTL (seconds)

Accept the default value of **300**.

6. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds.

To create an Amazon Route 53 alias record to route traffic to an Elastic Beanstalk environment

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Choose the name of the hosted zone that you want to use to route traffic to your Elastic Beanstalk environment.
4. Choose **Create record**.
5. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your Elastic Beanstalk environment. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use acme.example.com to route traffic to your environment, enter **acme**.

Value/Route traffic to

Choose **Alias to Elastic Beanstalk environment**, then choose the Region that the endpoint is from. Choose the domain name of the environment that you want to route traffic to. This is the value that you get when you perform the procedure in the topic [Getting the domain name for your Elastic Beanstalk environment \(p. 503\)](#).

If you used different accounts to create your Route 53 hosted zone and your Elastic Beanstalk environment, enter the CNAME attribute for the Elastic Beanstalk environment.

Record type

Accept the default, **A – IPv4 address**.

Evaluate target health

Accept the default value, **Yes**.

6. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your Elastic Beanstalk environment by using the name of the alias record that you create in this procedure.

Routing traffic to an ELB load balancer

If you host a website on multiple Amazon EC2 instances, you can distribute traffic to your website across the instances by using an Elastic Load Balancing (ELB) load balancer. The ELB service automatically scales the load balancer as traffic to your website changes over time. The load balancer also can monitor the health of its registered instances and route domain traffic only to healthy instances.

To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an [alias record](#) that points to your load balancer. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as example.com, and for subdomains, such as www.example.com. (You can create CNAME records only for subdomains.)

Note

Route 53 doesn't charge for alias queries to ELB load balancers or other AWS resources.

Prerequisites

Before you get started, you need the following:

- An ELB load balancer. You can use an ELB Classic, Application, or Network Load Balancer. For information about creating a load balancer, see [Getting started with Elastic Load Balancing](#) in the *Elastic Load Balancing User Guide*.

Give the load balancer a name that will help you remember what it's for later. The name that you specify when you create a load balancer is the name that you'll choose when you create an alias record in the Route 53 console.

- A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

For information about using Route 53 as the DNS service provider for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Configuring Amazon Route 53 to route traffic to an ELB load balancer

To configure Amazon Route 53 to route traffic to an ELB load balancer, perform the following procedure.

To route traffic to an ELB load balancer

1. If you created the Route 53 hosted zone and ELB load balancer using the same account, skip to step 2.
If you created the hosted zone and the ELB load balancer using different accounts, perform the procedure [Getting the DNS name for an ELB load balancer \(p. 393\)](#) to get the DNS name for the load balancer.
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Hosted zones**.
4. Choose the name of the hosted zone that has the domain name that you want to use to route traffic to your load balancer.
5. Choose **Create record**.
6. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain or subdomain name that you want to use to route traffic to your ELB load balancer. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use acme.example.com to route traffic to your load balancer, enter **acme**.

Alias

If you are using the **Quick create** record creation method, turn on **Alias**.

Value/Route traffic to

Choose **Alias to Application and Classic Load Balancer** or **Alias to Network Load Balancer**, then choose the Region that the endpoint is from.

If you created the hosted zone and the ELB load balancer using the same AWS account –
Choose the name that you assigned to the load balancer when you created it.

If you created the hosted zone and the ELB load balancer using different accounts – Enter the value that you got in step 1 of this procedure.

Note

The console prepends **dualstack.** to the DNS name of the Application and Classic Load Balancer from the same AWS account only. When a client, such as a web browser, requests the IP address for your domain name (example.com) or subdomain name (www.example.com), the client can request an IPv4 address (an A record), an IPv6 address (a AAAA record), or both IPv4 and IPv6 addresses (in separate requests with IPv4 first). The **dualstack.** designation allows Route 53 to respond with the appropriate IP address for your load balancer based on which IP address format the client requested. You will need to prepend **dualstack.** for Application and Classic Load Balancer from the different account.

Record type

Choose **A – IPv4 address**.

Evaluate target health

If you want Route 53 to route traffic based on the health of your resources, choose **Yes**. For more information about checking the health of your resources, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

7. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your load balancer by using the name of the alias record that you created in this procedure.

Routing traffic to a website that is hosted in an Amazon S3 bucket

Amazon Simple Storage Service (Amazon S3) provides secure, durable, highly scalable [cloud storage](#). You can configure an S3 bucket to host a static website that can include web pages and client-side scripts. (S3 doesn't support server-side scripting.)

To route domain traffic to an S3 bucket, use Amazon Route 53 to create an [alias record](#) that points to your bucket. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, except you can create an alias record both for the root domain, such as example.com, and for subdomains, such as www.example.com. You can create CNAME records only for subdomains.

Note

Route 53 doesn't charge for alias queries to S3 buckets or other AWS resources.

Prerequisites

Before you get started, you need the following. If you're new to Amazon Route 53 or S3, see [Getting started with Amazon Route 53 \(p. 17\)](#), which guides you through the entire process, including registering a domain name, and creating and configuring an S3 bucket.

- An S3 bucket that's configured to host a static website.

For more information, see [Configure a bucket for website hosting](#) in the *Amazon Simple Storage Service User Guide*.

Important

The bucket must have the same name as your domain or subdomain. For example, if you want to use the subdomain acme.example.com, the name of the bucket must be acme.example.com.

You can route traffic for a domain and its subdomains, such as example.com and www.example.com, to a single bucket. Create a bucket for the domain and each subdomain, and configure all but one of the buckets to redirect traffic to the remaining bucket. For more information, see [Getting started with Amazon Route 53 \(p. 17\)](#).

Note

An S3 bucket that's configured as a website endpoint doesn't support SSL/TLS, so you need to route traffic to the CloudFront distribution and use the S3 bucket as the origin for the distribution.

For instructions on how to create a CloudFront distribution, see [Create a CloudFront distribution](#) and [Configuring alternate domain names and HTTPS](#) in the *CloudFront User Guide*, as well as [Routing traffic to an Amazon CloudFront distribution by using your domain name \(p. 498\)](#).

- A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

For information about using Route 53 as the DNS service provider for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Configuring Amazon Route 53 to route traffic to an S3 Bucket

To configure Amazon Route 53 to route traffic to an S3 bucket that is configured to host a static website, perform the following procedure.

To route traffic to an S3 bucket

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Choose the name of the hosted zone that has the domain name that you want to use to route traffic to your S3 bucket.
4. Choose **Create record**.
5. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your S3 bucket. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use acme.example.com to route traffic to your bucket, enter **acme**.

Alias

If you are using the **Quick create** record creation method, turn on **Alias**.

Value/Route traffic to

Choose **Alias to S3 website endpoint**, then choose the Region that the endpoint is from.

Choose the bucket that has the same name that you specified for **Record name**.

The list includes a bucket only if the bucket meets the following requirements:

- The name of the bucket is the same as the name of the record that you're creating.
- The bucket is configured as a website endpoint.
- The bucket was created by the current AWS account.

If you created the bucket using a different AWS account, enter the name of the Region that you created your S3 bucket in. For the correct format for the Region name, see the **Website endpoint** column in the table [Amazon S3 website endpoints](#) in the *Amazon Web Services General Reference*.

Record type

Choose **A – IPv4 address**.

Evaluate target health

Accept the default value of **Yes**.

6. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your S3 bucket by using the name of the alias record that you created in this procedure.

Routing traffic to an Amazon Virtual Private Cloud interface endpoint by using your domain name

An Amazon Virtual Private Cloud (Amazon VPC) interface endpoint lets you use AWS PrivateLink to access selected services. These services include some AWS services, services that are hosted by other AWS customers and partners in their own VPCs, and supported AWS Marketplace partner services.

To route domain traffic to an interface endpoint, use Amazon Route 53 to create an alias record. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as example.com, and for subdomains, such as www.example.com. (You can create CNAME records only for subdomains.)

Last updated: 2013-04-01

Note

Route 53 doesn't charge for alias queries to interface endpoints or other AWS resources.

Topics

- [Prerequisites \(p. 510\)](#)
- [Configuring Amazon Route 53 to route traffic to an Amazon VPC interface endpoint \(p. 510\)](#)

Prerequisites

Before you get started, you need the following:

- An Amazon VPC interface endpoint. For more information, see [Interface VPC endpoints \(AWS PrivateLink\)](#) in the *Amazon VPC User Guide*.
- A registered domain name. You can use Amazon Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

For information about using Route 53 as the DNS service provider for your domain, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).

Configuring Amazon Route 53 to route traffic to an Amazon VPC interface endpoint

To configure Amazon Route 53 to route traffic to an Amazon VPC interface endpoint, perform the following procedure.

To route traffic to an Amazon VPC interface endpoint

1. If you created the Route 53 hosted zone and the Amazon VPC interface endpoint using the same account, skip to step 2.
If you created the hosted zone and the interface endpoint using different accounts, get the service name for the interface endpoint:
 - a. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. In the navigation pane, choose **Endpoints**.
 - c. In the right pane, choose the endpoint that you want to route internet traffic to.
 - d. In the bottom pane, get the value of DNS name, for example, `vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com`.
2. Open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Hosted zones**.
4. Choose the name of the hosted zone that has the domain name that you want to use to route traffic to your interface endpoint.
5. Choose **Create record**.
6. Specify the following values:

Routing policy

Choose the applicable routing policy. For more information, see [Choosing a routing policy \(p. 371\)](#).

Record name

Enter the domain name that you want to use to route traffic to your Amazon VPC interface endpoint.

Alias

If you are using the **Quick create** record creation method, turn on **Alias**.

Value/Route traffic to

Choose **Alias to VPC endpoint**, then choose the Region that the endpoint is from.

How you specify the value for **Endpoints** depends on whether you created the hosted zone and the interface endpoint using the same AWS account or different accounts:

- **Same account** – Choose the list, and find the category **Amazon VPC endpoints**. Then choose the DNS name of the interface endpoint that you want to route internet traffic to.
- **Different accounts** – Enter the value that you got in step 1 of this procedure.

Record type

Choose **A – IPv4 address**.

Evaluate target health

Accept the default value of **Yes**.

7. Choose **Create records**.

Changes generally propagate to all Route 53 servers within 60 seconds. When propagation is done, you'll be able to route traffic to your interface endpoint by using the name of the alias record that you created in this procedure.

Routing traffic to Amazon WorkMail

If you're using Amazon WorkMail for your business email and you're using Amazon Route 53 as your DNS service, you can use Route 53 to route traffic to your Amazon WorkMail email domain. The name of your Route 53 hosted zone (such as example.com) must match the name of an Amazon WorkMail domain.

Note

You can route traffic to an Amazon WorkMail domain only for public hosted zones.

To route traffic to Amazon WorkMail, perform the following four procedures.

To configure Amazon Route 53 as your DNS service and add an Amazon WorkMail organization and email domain

1. If you haven't registered the domain name that you want to use in your email addresses (such as john@example.com), register the domain now so you know that the domain is available. For more information, see [Registering a new domain \(p. 42\)](#).
If Amazon Route 53 is not the DNS service for the email domain that you added to Amazon WorkMail, migrate DNS service for the domain to Route 53. For more information, see [Making Amazon Route 53 the DNS service for an existing domain \(p. 325\)](#).
2. Add an Amazon WorkMail organization and email domain. For more information, see [Getting started for new users](#) in the *Amazon WorkMail Administrator Guide*.

To create a Route 53 TXT record for Amazon WorkMail

1. In the navigation pane of the Amazon WorkMail console, choose **Domains**.

2. Choose the name of the email domain, such as example.com, that you want to use to route traffic to Amazon WorkMail.
3. Open another browser tab, and open the [Route 53 console](#).
4. In the Route 53 console, do the following:
 - a. In the navigation pane, choose **Hosted zones**.
 - b. Choose the name of the hosted zone that you want to use for your Amazon WorkMail email domain.
5. In the Amazon WorkMail console, in the section **Step 1: Verify domain ownership**, go to the **Hostname** column, and copy the part of the value that precedes your email domain name.

For example, if your Amazon WorkMail email domain is **example.com** and the value of **Hostname** is **_amazones.example.com**, copy **_amazones**.
6. In the Route 53 console, do the following:
 - a. Choose **Create record**, and choose **Simple routing**.
 - b. For **Record name**, paste the value that you copied in step 5.
 - c. For **Record type**, choose **TXT – Text**.
7. In the Amazon WorkMail console, for the TXT record, copy the value of the **Value** column, including the quotation marks.
8. In the Route 53 console, do the following:
 - a. For **Value/Route traffic to**, choose **IP address or another value depending on the record type**, and paste the value that you copied in step 7.

Don't change any other settings.
 - b. Choose **Create**.

To create a Route 53 MX record for Amazon WorkMail

1. In the Amazon WorkMail console, in the section **Step 2: Finalize domain setup**, go to the row that has a **Record type** of **MX**, and copy the value of the **Value** column.
2. In the Route 53 console, do the following:
 - a. Choose **Create record**.
 - b. For **Value/Route traffic to**, choose **IP address or another value depending on the record type**, and paste the value that you copied in step 1.
 - c. For **Record type**, choose **MX – Mail Exchange**.

Don't change any other settings.
 - d. Choose **Create records**.

To create four Route 53 CNAME records for Amazon WorkMail

1. In the Amazon WorkMail console, in the section **Step 2: Finalize domain setup**, go to the first row that has a **Record type** of **CNAME**. In the **Hostname** column, copy the part of the value that precedes your email domain name.

For example, if your Amazon WorkMail email domain is **example.com** and the value of **Hostname** is **autodiscover.example.com**, copy **autodiscover**.
2. In the Route 53 console, do the following:
 - a. Choose **Create record**.

- b. For **Record name**, paste the value that you copied in step 1.
- c. For **Record type**, choose **CNAME – Canonical Name**.
3. In the Amazon WorkMail console, in the first row that has a **Record type** of **CNAME**, copy the value of the **Value** column.
4. In the Route 53 console, do the following:
 - a. For **Value/Route traffic to**, choose **IP address or another value depending on the record type**, and paste the value that you copied in step 3.

Don't change any other settings.
 - b. Choose **Create records**.
5. Repeat steps 1 through 4 for the remaining CNAME records that are listed in the Amazon WorkMail console.

Routing traffic to other AWS resources

The following list includes links to guidance in other guides on how to use Route 53 to route traffic to those services.

- [Using AWS Cloud Map](#) in the [AWS Cloud Map user guide](#).
- [Manage custom domains](#) in the [AWS App Runner developer guide](#).
- [Using Route 53 as a DNS provider](#) in the [AWS Transfer Family user guide](#).
- [Using Route 53 to point a domain to an Amazon Lightsail instance](#).

Creating Amazon Route 53 and Amazon Route 53 Resolver resources with AWS CloudFormation

Amazon Route 53 and Amazon Route 53 Resolver are integrated with AWS CloudFormation, a service that helps you to model and set up your AWS resources so that you can spend less time creating and managing your resources and infrastructure. You create a template that describes all the AWS resources that you want, and AWS CloudFormation provisions and configures those resources for you.

When you use AWS CloudFormation, you can reuse your template to set up your Route 53 and Route 53 Resolver resources consistently and repeatedly. Describe your resources once, and then provision the same resources over and over in multiple AWS accounts and Regions.

Route 53, Route 53 Resolver, and AWS CloudFormation templates

To provision and configure resources for Route 53, Route 53 Resolver, and related services, you must understand [AWS CloudFormation templates](#). Templates are formatted text files in JSON or YAML. These templates describe the resources that you want to provision in your AWS CloudFormation stacks. If you're unfamiliar with JSON or YAML, you can use AWS CloudFormation Designer to help you get started with AWS CloudFormation templates. For more information, see [What is AWS CloudFormation Designer?](#) in the [AWS CloudFormation User Guide](#).

Route 53 supports creating the following resource types in AWS CloudFormation:

- `AWS::Route53::DNSSEC`

- [AWS::Route53::HealthCheck](#)
- [AWS::Route53::HostedZone](#)
- [AWS::Route53::KeySigningKey](#)
- [AWS::Route53::RecordSet](#)
- [AWS::Route53::RecordSetGroup](#)

For more information, including examples of JSON and YAML templates for Route 53 resources, see the [Amazon Route 53 resource type reference](#) in the *AWS CloudFormation User Guide*.

Route 53 Resolver supports creating the following resource types in AWS 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](#)

For more information, including examples of JSON and YAML templates for Route 53 Resolver resources, see the [Amazon Route 53 Resolver resource type reference](#) in the *AWS CloudFormation User Guide*.

Learn more about AWS CloudFormation

To learn more about AWS CloudFormation, see the following resources:

- [AWS CloudFormation](#)
- [AWS CloudFormation User Guide](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation Command Line Interface User Guide](#)

Creating Amazon Route 53 health checks and configuring DNS failover

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following:

- The health of a specified resource, such as a web server.
- The status of other health checks.
- The status of an Amazon CloudWatch alarm.
- Additionally, with Amazon Route 53 Application Recovery Controller, you can set up routing control health checks with DNS failover records to manage traffic failover for your application. To learn more, see [Amazon Route 53 Application Recovery Controller Developer Guide](#).

For an overview of the types of health checks, see [Types of Amazon Route 53 health checks \(p. 516\)](#). For information about creating health checks, see [Creating and updating health checks \(p. 519\)](#).

After you create a health check, you can get the status of the health check, get notifications when the status changes, and configure DNS failover:

Getting health check status and notifications

You can view the current and recent status of your health checks on the Route 53 console. You can also work with health checks programmatically through one of the AWS SDKs, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the Route 53 API.

If you want to receive a notification when the status of a health check changes, you can configure an Amazon CloudWatch alarm for each health check.

For information about viewing health check status and receiving notifications, see [Monitoring health check status and getting notifications \(p. 530\)](#).

Configuring DNS failover

If you have multiple resources that perform the same function, you can configure DNS failover so that Route 53 will route your traffic from an unhealthy resource to a healthy resource. For example, if you have two web servers and one web server becomes unhealthy, Route 53 can route traffic to the other web server. For more information, see [Configuring DNS failover \(p. 536\)](#).

Topics

- [Types of Amazon Route 53 health checks \(p. 516\)](#)
- [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#)
- [Creating, updating, and deleting health checks \(p. 518\)](#)
- [Monitoring health check status and getting notifications \(p. 530\)](#)
- [Configuring DNS failover \(p. 536\)](#)
- [Naming and tagging health checks \(p. 551\)](#)

- [Using health checks with Amazon Route 53 API versions earlier than 2012-12-12 \(p. 553\)](#)

Types of Amazon Route 53 health checks

You can create the following types of Amazon Route 53 health checks:

Health checks that monitor an endpoint

You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name. At regular intervals that you specify, Route 53 submits automated requests over the internet to your application, server, or other resource to verify that it's reachable, available, and functional. Optionally, you can configure the health check to make requests similar to those that your users make, such as requesting a web page from a specific URL.

Health checks that monitor other health checks (calculated health checks)

You can create a health check that monitors whether Route 53 considers other health checks healthy or unhealthy. One situation where this might be useful is when you have multiple resources that perform the same function, such as multiple web servers, and your chief concern is whether some minimum number of your resources are healthy. You can create a health check for each resource without configuring notification for those health checks. Then you can create a health check that monitors the status of the other health checks and that notifies you only when the number of available web resources drops below a specified threshold.

Health checks that monitor CloudWatch alarms

You can create CloudWatch alarms that monitor the status of CloudWatch metrics, such as the number of throttled read events for an Amazon DynamoDB database or the number of Elastic Load Balancing hosts that are considered healthy. After you create an alarm, you can create a health check that monitors the same data stream that CloudWatch monitors for the alarm.

To improve resiliency and availability, Route 53 doesn't wait for the CloudWatch alarm to go into the ALARM state. The status of a health check changes from healthy to unhealthy based on the data stream and on the criteria in the CloudWatch alarm.

Amazon Route 53 Application Recovery Controller

Amazon Route 53 Application Recovery Controller gives you insights into whether your applications and resources are ready for recovery, and helps you manage and coordinate failover. Health checks in Route 53 ARC are associated with routing controls, which are simple on/off switches. You configure each routing control health check with a failover DNS record. Then you can simply update your routing controls in Route 53 ARC to reroute traffic and fail over your applications, for example, across Availability Zones or AWS-Regions. For more information, see [Amazon Route 53 Application Recovery Controller Developer Guide](#).

To learn more about readiness checks, see [Readiness check in Route 53 ARC](#), and to learn more about routing controls, see [Routing control in Route 53 ARC](#) in the Route 53 ARC developer guide.

How Amazon Route 53 determines whether a health check is healthy

The method that Amazon Route 53 uses to determine whether a health check is healthy depends on the type of health check.

Topics

- [How Route 53 determines the status of health checks that monitor an endpoint \(p. 517\)](#)
- [How Route 53 determines the status of health checks that monitor other health checks \(p. 518\)](#)
- [How Route 53 determines the status of health checks that monitor CloudWatch alarms \(p. 518\)](#)

How Route 53 determines the status of health checks that monitor an endpoint

Route 53 has health checkers in locations around the world. When you create a health check that monitors an endpoint, health checkers start to send requests to the endpoint that you specify to determine whether the endpoint is healthy. You can choose which locations you want Route 53 to use, and you can specify the interval between checks: every 10 seconds or every 30 seconds. Note that Route 53 health checkers in different data centers don't coordinate with one another, so you'll sometimes see several requests per second regardless of the interval you chose, followed by a few seconds with no health checks at all.

Each health checker evaluates the health of the endpoint based on two values:

- Response time. A resource can be slow to respond or can fail to respond to a health check request for a variety of reasons. For example, the resource is shut down for maintenance, it's under a distributed denial of service (DDoS) attack, or the network is down.
- Whether the endpoint responds to a number of consecutive health checks that you specify (the failure threshold)

Route 53 aggregates the data from the health checkers and determines whether the endpoint is healthy:

- If more than 18% of health checkers report that an endpoint is healthy, Route 53 considers it healthy.
- If 18% of health checkers or fewer report that an endpoint is healthy, Route 53 considers it unhealthy.

The 18% value was chosen to ensure that health checkers in multiple regions consider the endpoint healthy. This prevents an endpoint from being considered unhealthy only because network conditions have isolated the endpoint from some health-checking locations. This value might change in a future release.

The response time that an individual health checker uses to determine whether an endpoint is healthy depends on the type of health check:

- **HTTP and HTTPS health checks** – Route 53 must be able to establish a TCP connection with the endpoint within four seconds. In addition, the endpoint must respond with an HTTP status code of 2xx or 3xx within two seconds after connecting.

Note

HTTPS health checks don't validate SSL/TLS certificates, so checks don't fail if a certificate is invalid or expired.

- **TCP health checks** – Route 53 must be able to establish a TCP connection with the endpoint within ten seconds.
- **HTTP and HTTPS health checks with string matching** – As with HTTP and HTTPS health checks, Route 53 must be able to establish a TCP connection with the endpoint within four seconds, and the endpoint must respond with an HTTP status code of 2xx or 3xx within two seconds after connecting.

After a Route 53 health checker receives the HTTP status code, it must receive the response body from the endpoint within the next two seconds. Route 53 searches the response body for a string that you specify. The string must appear entirely in the first 5,120 bytes of the response body or the endpoint fails the health check. If you're using the Route 53 console, you specify the string in the **Search String**

field. If you're using the Route 53 API, you specify the string in the `SearchString` element when you create the health check.

For health checks that monitor an endpoint (except TCP health checks), if the response from the endpoint includes any headers, the headers must be in the format that is defined in RFC7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, [section 3.2, "Header Fields."](#)

Route 53 considers a new health check to be healthy until there's enough data to determine the actual status, healthy or unhealthy. If you chose the option to invert the health check status, Route 53 considers a new health check to be *unhealthy* until there's enough data.

How Route 53 determines the status of health checks that monitor other health checks

A health check can monitor the status of other health checks; this type of health check is known as a *calculated health check*. The health check that does the monitoring is the *parent health check*, and the health checks that are monitored are *child health checks*. One parent health check can monitor the health of up to 255 child health checks. Here's how the monitoring works:

- Route 53 adds up the number of child health checks that are considered to be healthy.
- Route 53 compares that number with the number of child health checks that must be healthy for the status of the parent health check to be considered healthy.

For more information, see [Monitoring other health checks \(calculated health checks\) \(p. 522\)](#) in [Values that you specify when you create or update health checks \(p. 519\)](#).

Route 53 considers a new health check to be healthy until there's enough data to determine the actual status, healthy or unhealthy. If you chose the option to invert the health check status, Route 53 considers a new health check to be *unhealthy* until there's enough data.

How Route 53 determines the status of health checks that monitor CloudWatch alarms

When you create a health check that is based on a CloudWatch alarm, Route 53 monitors the data stream for the corresponding alarm instead of monitoring the alarm state. If the data stream indicates that the state of the alarm is **OK**, the health check is considered healthy. If the data stream indicates that the state is **Alarm**, the health check is considered unhealthy. If the data stream doesn't provide enough information to determine the state of the alarm, the health check status depends on the setting for **Health check status**: healthy, unhealthy, or last known status. (In the Route 53 API, this setting is `InsufficientDataHealthStatus`.)

Note

Because Route 53 health checks monitor CloudWatch data streams instead of the state of CloudWatch alarms, you can't force the status of a health check to change by using the CloudWatch [SetAlarmState](#) API operation.

Route 53 considers a new health check to be healthy until there's enough data to determine the actual status, healthy or unhealthy. If you chose the option to invert the health check status, Route 53 considers a new health check to be *unhealthy* until there's enough data.

Creating, updating, and deleting health checks

The procedures in the following topics explain how to create, update, and delete Route 53 health checks.

Important

If you're updating or deleting health checks that are associated with records, review the tasks in [Updating or deleting health checks when DNS failover is configured \(p. 529\)](#) before you proceed.

Topics

- [Creating and updating health checks \(p. 519\)](#)
- [Values that you specify when you create or update health checks \(p. 519\)](#)
- [Values that Amazon Route 53 displays when you create a health check \(p. 528\)](#)
- [Updating health checks when you change CloudWatch alarm settings \(health checks that monitor a CloudWatch alarm only\) \(p. 528\)](#)
- [Deleting health checks \(p. 528\)](#)
- [Updating or deleting health checks when DNS failover is configured \(p. 529\)](#)
- [Configuring router and firewall rules for Amazon Route 53 health checks \(p. 529\)](#)

Creating and updating health checks

The following procedure describes how to create and update health checks using the Route 53 console.

To create or update a health check (console)

1. If you're updating health checks that are already associated with records, perform the recommended tasks in [Updating or deleting health checks when DNS failover is configured \(p. 529\)](#).
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Health Checks**.
4. If you want to update an existing health check, select the health check, and then choose **Edit Health Check**.

If you want to create a health check, choose **Create Health Check**. For more information about each setting, move the mouse pointer over a label to see its tooltip.

5. Enter the applicable values. Note that some values can't be changed after you create a health check. For more information, see [Values that you specify when you create or update health checks \(p. 519\)](#).
6. Choose **Create Health Check**.

Note

Route 53 considers a new health check to be healthy until there's enough data to determine the actual status, healthy or unhealthy. If you chose the option to invert the health check status, Route 53 considers a new health check to be *unhealthy* until there's enough data.

7. Associate the health check with one or more Route 53 records. For information about creating and updating records, see [Working with records \(p. 370\)](#).

Values that you specify when you create or update health checks

When you create or update health checks, you specify the applicable values. Note that you can't change some values after you create a health check.

Topics

- [Monitoring an endpoint \(p. 520\)](#)
- [Monitoring other health checks \(calculated health checks\) \(p. 522\)](#)
- [Monitoring a CloudWatch alarm \(p. 523\)](#)
- [Advanced configuration \("Monitor an Endpoint" only\) \(p. 525\)](#)
- [Get notified when a health check fails \(p. 527\)](#)

Name

Optional, but recommended: The name that you want to assign to the health check. If you specify a value for **Name**, Route 53 adds a tag to the health check, assigns the value **Name** to the tag key, and assigns the value that you specify to the tag value. The value of the **Name** tag appears in the list of health checks in the Route 53 console, which lets you easily distinguish health checks from one another.

For more information about tagging and health checks, see [Naming and tagging health checks \(p. 551\)](#).

What to monitor

Whether you want this health check to monitor an endpoint or the status of other health checks:

- **Endpoint** – Route 53 monitors the health of an endpoint that you specify. You can specify the endpoint by providing either a domain name or an IP address and a port.

Note

If you specify a non-AWS endpoint, an additional charge applies. For more information, including a definition of AWS endpoints, see "Health Checks" on the [Route 53 Pricing](#) page.

- **Status of other health checks (calculated health check)** – Route 53 determines whether this health check is healthy based on the status of other health checks that you specify. You also specify how many of the health checks need to be healthy for this health check to be considered healthy.
- **State of CloudWatch alarm** – Route 53 determines whether this health check is healthy by monitoring the data stream for a CloudWatch alarm.

Monitoring an endpoint

If you want this health check to monitor an endpoint, specify the following values:

- [Specify endpoint by](#)
- [Protocol](#)
- [IP address](#)
- [Host name](#)
- [Port](#)
- [Domain name](#)
- [Path](#)

Specify endpoint by

Whether you want to specify the endpoint using an IP address or using a domain name.

After you create a health check, you can't change the value of **Specify endpoint by**.

Protocol

The method that you want Route 53 to use to check the health of your endpoint:

- **HTTP** – Route 53 tries to establish a TCP connection. If successful, Route 53 submits an HTTP request and waits for an HTTP status code of 2xx or 3xx.
- **HTTPS** – Route 53 tries to establish a TCP connection. If successful, Route 53 submits an HTTPS request and waits for an HTTP status code of 2xx or 3xx.

Important

If you choose **HTTPS**, the endpoint must support TLS v1.0 or later.

If you choose **HTTPS** for the value of **Protocol**, an additional charge applies. For more information, see [Route 53 Pricing](#).

- **TCP** – Route 53 tries to establish a TCP connection.

For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

After you create a health check, you can't change the value of **Protocol**.

IP address ("Specify endpoint by IP address" Only)

The IPv4 or IPv6 address of the endpoint on which you want Route 53 to perform health checks, if you chose **Specify endpoint by IP address**.

Route 53 cannot check the health of endpoints for which the IP address is in local, private, nonroutable, or multicast ranges. For more information about IP addresses that you can't create health checks for, see the following documents:

- [RFC 5735, Special Use IPv4 Addresses](#)
- [RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space](#).
- [RFC 5156, Special-Use IPv6 Addresses](#)

If the endpoint is an Amazon EC2 instance, we recommend that you create an Elastic IP address, associate it with your EC2 instance, and specify the Elastic IP address. This ensures that the IP address of your instance will never change. For more information, see [Elastic IP addresses \(EIP\)](#) in the [Amazon EC2 User Guide for Linux Instances](#).

If you delete the Amazon EC2 instance, make sure you also delete the health check associated to the EIP. For more information, see [Best practices for Elastic IP addresses for health checks \(p. 670\)](#).

Note

If you specify a non-AWS endpoint, an additional charge applies. For more information, including a definition of AWS endpoints, see "Health Checks" on the [Route 53 Pricing](#) page.

Host name ("Specify endpoint by IP address" Only, HTTP and HTTPS Protocols Only)

The value that you want Route 53 to pass in the `Host` header in HTTP and HTTPS health checks. This is typically the fully qualified DNS name of the website on which you want Route 53 to perform health checks. When Route 53 checks the health of an endpoint, here is how it constructs the `Host` header:

- If you specify a value of **80** for **Port** and **HTTP** for **Protocol**, Route 53 passes to the endpoint a `Host` header that contains the value of **Host name**.
- If you specify a value of **443** for **Port** and **HTTPS** for **Protocol**, Route 53 passes to the endpoint a `Host` header that contains the value of **Host name**.
- If you specify another value for **Port** and either **HTTP** or **HTTPS** for **Protocol**, Route 53 passes to the endpoint a `Host` header that contains the value `Host name:Port`.

If you choose to specify the endpoint by IP address and you don't specify a value for **Host name**, Route 53 substitutes the value of **IP address** in the `Host` header in each of the preceding cases.

Port

The port on the endpoint on which you want Route 53 to perform health checks.

Domain name ("Specify endpoint by domain name" Only, All Protocols)

The domain name (example.com) or subdomain name (backend.example.com) of the endpoint that you want Route 53 to perform health checks on, if you choose **Specify endpoint by domain name**.

If you choose to specify the endpoint by domain name, Route 53 sends a DNS query to resolve the domain name that you specify in **Domain name** at the interval that you specify in **Request interval**. Using an IP address that DNS returns, Route 53 then checks the health of the endpoint.

Note

If you specify the endpoint by domain name, Route 53 uses only IPv4 to send health checks to the endpoint. If there's no record with a type of A for the name that you specify for **Domain name**, the health check fails with a "DNS resolution failed" error.

If you want to check the health of failover, geolocation, geoproximity, latency, multivalue, or weighted records, and you choose to specify the endpoint by domain name, we recommend that you create a separate health check for each endpoint. For example, create a health check for each HTTP server that is serving content for www.example.com. For the value of **Domain name**, specify the domain name of the server (such as us-east-2-www.example.com), not the name of the records (www.example.com).

Important

In this configuration, if you create a health check for which the value of **Domain name** matches the name of the records and then associate the health check with those records, health check results will be unpredictable.

In addition, if the value of **Protocol** is **HTTP** or **HTTPS**, Route 53 passes the value of **Domain name** in the **Host** header as described in **Host name**, earlier in this list. If the value of **Protocol** is **TCP**, Route 53 doesn't pass a **Host** header.

Note

If you specify a non-AWS endpoint, an additional charge applies. For more information, including a definition of AWS endpoints, see "Health Checks" on the [Route 53 Pricing](#) page.

Path (HTTP and HTTPS Protocols Only)

The path that you want Route 53 to request when performing health checks. The path can be any value for which your endpoint will return an HTTP status code of 2xx or 3xx when the endpoint is healthy, such as the file /docs/route53-health-check.html. You can also include query string parameters, for example, /welcome.html?language=jp&login=y. If you don't include a leading slash (/) character, Route 53 automatically adds one.

Monitoring other health checks (calculated health checks)

If you want this health check to monitor the status of other health checks, specify the following values:

- [Health checks to monitor](#)
- [Report healthy when](#)
- [Invert health check status](#)
- [Disabled](#)

Health checks to monitor

The health checks that you want Route 53 to monitor to determine the health of this health check.

You can add up to 256 health checks to **Health checks to monitor**. To remove a health check from the list, choose the x at the right of the highlight for that health check.

Note

You can't configure a calculated health check to monitor the health of other calculated health checks.

If you disable a health check that a calculated health check is monitoring, Route 53 considers the disabled health check to be healthy as it calculates whether the calculated health check is healthy. If you want the disabled health check to be considered unhealthy, choose the **Invert health check status** check box.

Report healthy when

The calculation that you want Route 53 to perform to determine whether this health check is healthy:

- **Report healthy when at least x of y selected health checks are healthy** – Route 53 considers this health check to be healthy when the specified number of health checks that you added to **Health checks to monitor** are healthy. Note the following:
 - If you specify a number greater than the number of health checks in **Health checks to monitor**, Route 53 always considers this health check to be unhealthy.
 - If you specify **0**, Route 53 always considers this health check to be healthy.
- **Report healthy when all health checks are healthy (AND)** – Route 53 considers this health check to be healthy only when all the health checks that you added to **Health checks to monitor** are healthy.
- **Report healthy when one or more health checks are healthy (OR)** – Route 53 considers this health check to be healthy when at least one of the health checks that you added to **Health checks to monitor** is healthy.

Invert health check status

Choose whether you want Route 53 to invert the status of a health check. If you choose this option, Route 53 considers health checks to be unhealthy when the status is healthy and vice versa.

Disabled

Stops Route 53 from performing health checks. When you disable a health check, Route 53 stops aggregating the status of the referenced health checks.

After you disable a health check, Route 53 considers the status of the health check to always be healthy. If you configured DNS failover, Route 53 continues to route traffic to the corresponding resources. If you want to stop routing traffic to a resource, change the value of [Invert health check status](#).

Note

Charges for a health check still apply when the health check is disabled.

Monitoring a CloudWatch alarm

If you want this health check to monitor the alarm state of a CloudWatch alarm, specify the following values:

- [CloudWatch alarm](#)
- [Health check status](#)
- [Invert health check status](#)
- [Disabled](#)

CloudWatch alarm

Choose the CloudWatch alarm that you want Route 53 to use to determine whether this health check is healthy.

Note

Route 53 supports CloudWatch alarms with the following features:

- Standard-resolution metrics. High-resolution metrics aren't supported. For more information, see [High-resolution metrics](#) in the *Amazon CloudWatch User Guide*.
- Statistics: Average, Minimum, Maximum, Sum, and SampleCount. Extended statistics aren't supported.
- Route 53 does not support "M out of N" alarms. For more information, see [Evaluating an alarm](#) in the *Amazon CloudWatch guide*.

Route 53 does not support alarms that use [metric math](#) to query multiple CloudWatch metrics.

If you want to create an alarm, perform the following steps:

1. Choose **create**. The CloudWatch console appears in a new browser tab.
2. Enter the applicable values. For more information, see [Create or edit a CloudWatch alarm](#) in the *Amazon CloudWatch User Guide*.
3. Return to the browser tab that the Route 53 console appears in.
4. Choose the refresh button next to the **CloudWatch alarm** list.
5. Choose the new alarm from the list.

Important

If you change settings for the CloudWatch alarm after you create a health check, you must update the health check. For more information, see [Updating health checks when you change CloudWatch alarm settings \(health checks that monitor a CloudWatch alarm only\)](#) (p. 528).

Health check status

Choose the status of the health check (healthy, unhealthy, or last known status) when CloudWatch has insufficient data to determine the state of the alarm that you chose for **CloudWatch alarm**. If you choose to use the last known status, Route 53 uses the status of the health check from the last time that CloudWatch had sufficient data to determine the alarm state. For new health checks that have no last known status, the default status for the health check is healthy.

The value of **Health check status** provides a temporary status when the data stream for a CloudWatch metric is briefly unavailable. (Route 53 monitors data streams for CloudWatch metrics, not the state of the corresponding alarm.) If the metric will be unavailable frequently or for long periods (longer than a few hours), we recommend that you not use the last known status.

Invert health check status

Choose whether you want Route 53 to invert the status of a health check. If you choose this option, Route 53 considers health checks to be unhealthy when the status is healthy and vice versa.

Disabled

Stops Route 53 from performing health checks. When you disable a health check, Route 53 stops monitoring the corresponding CloudWatch metrics.

After you disable a health check, Route 53 considers the status of the health check to always be healthy. If you configured DNS failover, Route 53 continues to route traffic to the corresponding resources. If you want to stop routing traffic to a resource, change the value of [Invert health check status](#).

Note

Charges for a health check still apply when the health check is disabled.

Advanced configuration ("Monitor an Endpoint" only)

If you choose the option to monitor an endpoint, you can also specify the following settings:

- Request interval
- Failure threshold
- String matching
- Search string
- Latency graphs
- Enable SNI
- Health checker regions
- Invert health check status
- Disabled

Request interval

The number of seconds between the time that each Route 53 health checker gets a response from your endpoint and the time that it sends the next health check request. If you choose an interval of 30 seconds, each of the Route 53 health checkers in data centers around the world will send your endpoint a health check request every 30 seconds. On average, your endpoint will receive a health check request about every two seconds. If you choose an interval of 10 seconds, the endpoint will receive a request more than once per second.

Note that Route 53 health checkers in different data centers don't coordinate with one another, so you'll sometimes see several requests per second regardless of the interval you chose, followed by a few seconds with no health checks at all.

After you create a health check, you can't change the value of **Request interval**.

Note

If you choose **Fast (10 seconds)** for the value of **Request interval**, an additional charge applies. For more information, see [Route 53 Pricing](#).

Failure threshold

The number of consecutive health checks that an endpoint must pass or fail for Route 53 to change the current status of the endpoint from unhealthy to healthy or vice versa. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

String matching (HTTP and HTTPS Only)

Whether you want Route 53 to determine the health of an endpoint by submitting an HTTP or HTTPS request to the endpoint and searching the response body for a specified string. If the response body contains the value that you specify in **Search string**, Route 53 considers the endpoint healthy. If not, or if the endpoint doesn't respond, Route 53 considers the endpoint unhealthy. The search string must appear entirely within the first 5,120 bytes of the response body.

After you create a health check, you can't change the value of **String matching**.

Note

If you choose **Yes** for the value of **String matching**, an additional charge applies. For more information, see [Route 53 Pricing](#).

How health checkers handle a compressed response

If the endpoint is a web server that returns a response that is compressed, the Route 53 health checker will uncompress the response before checking for the specified search string only if the web server compressed the response using a compression algorithm that health checkers support. Health checkers support the following compression algorithms:

- Gzip
- Deflate

If the response is compressed using another algorithm, the health checker can't decompress the response before searching for the string. In this case, the search will almost always fail, and Route 53 will consider the endpoint unhealthy.

Search string (Only When "String matching" Is Enabled)

The string that you want Route 53 to search for in the body of the response from your endpoint. The maximum length is 255 characters.

Route 53 considers case when searching for **Search string** in the response body.

Latency graphs

Choose whether you want Route 53 to measure the latency between health checkers in multiple AWS Regions and your endpoint. If you choose this option, CloudWatch latency graphs appear on the **Latency** tab on the **Health checks** page in the Route 53 console. If Route 53 health checkers can't connect to the endpoint, Route 53 can't display latency graphs for that endpoint.

After you create a health check, you can't change the value of **Latency measurements**.

Note

If you configure Route 53 to measure the latency between health checkers and your endpoint, an additional charge applies. For more information, see [Route 53 Pricing](#).

Enable SNI (HTTPS Only)

Specify whether you want Route 53 to send the host name to the endpoint in the `client_hello` message during TLS negotiation. This allows the endpoint to respond to the HTTPS request with the applicable SSL/TLS certificate.

Some endpoints require that HTTPS requests include the host name in the `client_hello` message. If you don't enable SNI, the status of the health check will be `SSL_alert_handshake_failure`. A health check can also have that status for other reasons. If SNI is enabled and you're still getting the error, check the SSL/TLS configuration on your endpoint and confirm that your certificate is valid.

Note the following requirements:

- The endpoint must support SNI.
- The SSL/TLS certificate on your endpoint includes a domain name in the `Common Name` field and possibly several more in the `Subject Alternative Names` field. One of the domain names in the certificate must match the value that you specify for **Host name**.

Health checker regions

Choose whether you want Route 53 to check the health of the endpoint by using health checkers in the recommended regions or by using health checkers in regions that you specify.

If you update a health check to remove a region that has been performing health checks, Route 53 continues to perform checks from that region for up to an hour. This ensures that some health checkers are always checking the endpoint (for example, if you replace three regions with four different regions).

If you choose **Customize**, choose the **x** for a region to remove it. Click the space at the bottom of the list to add a region back to the list. You must specify at least three regions.

Invert health check status

Choose whether you want Route 53 to invert the status of a health check. If you choose this option, Route 53 considers health checks to be unhealthy when the status is healthy and vice versa. For example, you might want Route 53 to consider a health check *unhealthy* if you configure string matching and the endpoint returns a specified value. For more information about health checks that perform string matching, see [String matching](#).

Disabled

Stops Route 53 from performing health checks. When you disable a health check, Route 53 stops trying to establish a TCP connection with the endpoint.

After you disable a health check, Route 53 considers the status of the health check to always be healthy. If you configured DNS failover, Route 53 continues to route traffic to the corresponding resources. If you want to stop routing traffic to a resource, change the value of [Invert health check status](#).

Note

Charges for a health check still apply when the health check is disabled.

Get notified when a health check fails

Use the following options to configure email notification when a health check fails:

- [Create alarm](#)
- [Send notification to](#)
- [Topic name](#)
- [Recipient email addresses](#)

Create alarm (Only When Creating Health Checks)

Specify whether you want to create a default CloudWatch alarm. If you choose **Yes**, CloudWatch sends you an Amazon SNS notification when the status of this endpoint changes to unhealthy and Route 53 considers the endpoint unhealthy for one minute.

Note

If you want CloudWatch to send you another Amazon SNS notification when the status changes back to healthy, you can create another alarm after you create the health check. For more information, see [Creating Amazon CloudWatch alarms](#) in the *Amazon CloudWatch User Guide*.

If you want to create an alarm for an existing health check or you want to receive notifications when Route 53 considers the endpoint unhealthy for more or less than one minute (the default value), select **No**, and add an alarm after you create the health check. For more information, see [Monitoring health checks using CloudWatch \(p. 532\)](#).

Send notification to (Only When Creating an Alarm)

Specify whether you want CloudWatch to send notifications to an existing Amazon SNS topic or to a new one:

- **Existing SNS topic** – Select the name of the topic from the list. The topic must be in the US East (N. Virginia) Region.
- **New SNS topic** – Enter a name for the topic in **Topic name**, and enter the email addresses that you want to send notifications to in **Recipients**. Separate multiple addresses with commas (,), semicolons (;), or spaces.

Route 53 will create the topic in the US East (N. Virginia) Region.

Topic name (Only When Creating a New SNS Topic)

If you specified **New SNS Topic**, enter the name of the new topic.

Recipient email addresses (Only When Creating a New SNS Topic)

If you specified **New SNS topic**, enter the email addresses that you want to send notifications to. Separate multiple names with commas (,), semicolons (;), or spaces.

Values that Amazon Route 53 displays when you create a health check

The [Create Health Check](#) page displays the following values based on the values that you typed:

URL

Either the full URL (for HTTP or HTTPS health checks) or the IP address and port (for TCP health checks) to which Route 53 will send requests when performing health checks.

Health Check Type

Either **Basic** or **Basic + additional options** based on the settings that you specified for this health check. For information about pricing for the additional options, see [Route 53 Pricing](#).

Updating health checks when you change CloudWatch alarm settings (health checks that monitor a CloudWatch alarm only)

If you create a Route 53 health check that monitors the data stream for a CloudWatch alarm and then you update the settings in the CloudWatch alarm, Route 53 doesn't automatically update the alarm settings in the health check. If you want the health check to start using the new alarm settings, you need to update the health check.

Note

To update a health check programmatically, you can use the `UpdateHealthCheck` API. Just specify the current values for `AlarmIdentifier` and `Region`, and Route 53 will get the latest settings from CloudWatch. For more information, see [UpdateHealthCheck](#) in the *Amazon Route 53 API Reference*.

To update a health check with new CloudWatch alarm settings (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. Select the check box for the health check that you want to update.
4. Choose **Edit health check**.

A note explains that the CloudWatch alarm for the health check has changed. The **Details** field shows the new alarm settings.

5. Choose **Save**.

Deleting health checks

To delete health checks, perform the following procedure.

Note

If you're using AWS Cloud Map and you configured AWS Cloud Map to create a Route 53 health check when you register an instance, you can't use the Route 53 console to delete the health check. The health check is deleted automatically when you deregister the instance. There can be a delay of several hours before the health check no longer appears in the Route 53 console.

To delete a health check (console)

1. If you're deleting health checks that are associated with records, perform the recommended tasks in [Updating or deleting health checks when DNS failover is configured \(p. 529\)](#).
2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
3. In the navigation pane, choose **Health Checks**.
4. In the right pane, select the health check that you want to delete.
5. Choose **Delete Health Check**.
6. Choose **Yes, Delete** to confirm.

Updating or deleting health checks when DNS failover is configured

When you want to update or delete health checks that are associated with records, or you want to change records that have associated health checks, you must consider how your changes affect routing of DNS queries and your DNS failover configuration.

Important

Route 53 doesn't prevent you from deleting a health check even if the health check is associated with one or more records. If you delete a health check and you don't update the associated records, the future status of the health check can't be predicted and might change. This will affect the routing of DNS queries for your DNS failover configuration.

To update or delete health checks that are already associated with records, we recommend that you perform the following tasks:

1. Identify the records that are associated with the health checks. To identify the records that are associated with a health check, you must do one of the following:
 - Review the records in each hosted zone using the Route 53 console. For more information, see [Listing records \(p. 441\)](#).
 - Run the `ListResourceRecordSets` API action on each hosted zone and review the response. For more information, see [ListResourceRecordSets](#) in the *Amazon Route 53 API Reference*.
2. Assess the change in behavior that will result from updating or deleting health checks, or from updating records. Based on that assessment, determine which changes to make.

For more information, see [What happens when you omit health checks? \(p. 544\)](#)
3. Change health checks and records as applicable. For more information, see the following topics:
 - [Creating and updating health checks \(p. 519\)](#)
 - [Editing records \(p. 440\)](#)
4. Delete the health checks that you're no longer using, if any. For more information, see [Deleting health checks \(p. 528\)](#).

Configuring router and firewall rules for Amazon Route 53 health checks

When Route 53 checks the health of an endpoint, it sends an HTTP, HTTPS, or TCP request to the IP address and port that you specified when you created the health check. For a health check to succeed, your router and firewall rules must allow inbound traffic from the IP addresses that the Route 53 health

checkers use. (In Amazon EC2, security groups act as firewalls. For more information, see [Amazon EC2 security groups](#) in the *Amazon EC2 User Guide for Linux Instances*.)

For the current list of IP addresses for Route 53 health checkers, for Route 53 name servers, and for other AWS services, see [IP address ranges of Amazon Route 53 servers \(p. 654\)](#).

Important

When you add IP addresses to a list of allowed IP addresses, add all the IP addresses in the CIDR range for each AWS Region that you specified when you created health checks, as well as the Global CIDR range. You might see that health check requests come from just one IP address in a Region. However, that IP address can change at any time to another of the IP addresses for that Region.

If you want to make sure that you include both the current and older health checker IP addresses, add ALL /26 and /18 IP address ranges to the allow list. For a complete list, see [AWS IP address ranges](#) in the *AWS General Reference*.

Monitoring health check status and getting notifications

You monitor the status of your health checks on the Amazon Route 53 console. You can also set CloudWatch alarms and get automated notifications when the status of your health check status changes.

Topics

- [Viewing health check status and the reason for health check failures \(p. 530\)](#)
- [Monitoring the latency between health checkers and your endpoint \(p. 531\)](#)
- [Monitoring health checks using CloudWatch \(p. 532\)](#)

Viewing health check status and the reason for health check failures

On the Route 53 console, you can view the status (healthy or unhealthy) of your health checks as reported by Route 53 health checkers. For all health checks except calculated health checks, you can also view the reason for the last health check failure, for example, health checkers were unable to establish a connection with the endpoint.

To view the status and last failure reason for a health check (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. For an overview of the status of all of your health checks—healthy or unhealthy—view the **Status** column. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).
4. For all health checks except calculated health checks, you can view the status of the Route 53 health checkers that are checking the health of a specified endpoint. Select the health check.
5. In the bottom pane, choose the **Health Checkers** tab.

Note

New health checks must propagate to Route 53 health checkers before the health check status and last failure reason appear in the **Status** column. Until propagation has finished, the message in that column explains that no status is available.

6. Choose whether you want to view the current status of the health check, or view the date and time of the last failure and the reason for the failure. The table on the **Status** tab includes the following values:

Health checker IP

The IP address of the Route 53 health checker that performed the health check.

Last checked

The date and time of the health check or the date and time of the last failure, depending on the option that you select at the top of the **Status** tab.

Status

Either the current status of the health check or the reason for the last health check failure, depending on the option that you select at the top of the **Status** tab.

Monitoring the latency between health checkers and your endpoint

When you create a health check, if you choose to monitor the status of an endpoint (not the status of other health checks) and you choose the **Latency graphs** option, you can view the following values on CloudWatch graphs on the Route 53 console:

- The average time, in milliseconds, that it took Route 53 health checkers to establish a TCP connection with the endpoint
- The average time, in milliseconds, that it took Route 53 health checkers to receive the first byte of the response to an HTTP or HTTPS request
- The average time, in milliseconds, that it took Route 53 health checkers to complete the SSL/TLS handshake

Note

You can't enable latency monitoring for existing health checks.

Important

The health checkers are run on 16 redundant availability zones. Occasionally an availability zone can be unavailable because of deployments, updates, maintenance, and so on. The health check system is designed to account for this without any customer impact.

To view the latency between Route 53 health checkers and your endpoint (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. Select the rows for the applicable health checks. You can view latency data only for health checks that monitor the status of an endpoint and for which the **Latency graphs** option is enabled.
4. In the bottom pane, choose the **Latency** tab.
5. Choose the time range and the geographic region that you want to display latency graphs for.

The graphs display the status for the specified time range:

TCP connection time (HTTP and TCP only)

The average time, in milliseconds, that it took Route 53 health checkers in the selected geographic region to establish a TCP connection with the endpoint.

Time to first byte (HTTP and HTTPS only)

The average time, in milliseconds, that it took Route 53 health checkers in the selected geographic region to receive the first byte of the response to an HTTP or HTTPS request.

Time to complete SSL handshake (HTTPS only)

The average time, in milliseconds, that it took Route 53 health checkers in the selected geographic region to complete the SSL/TLS handshake.

Note

If you select more than one health check, the graph displays a separate color-coded line for each health check.

6. To view a larger graph and specify different settings, click the graph. You can change the following settings:

Statistic

Changes the calculation that CloudWatch performs on the data.

Time range

Displays the status of a health check over a different period, for example, overnight or last week.

Period

Changes the interval between data points in the graph.

Note the following:

- If you just created a health check, you might need to wait for a few minutes for data to appear in the graph and for the health check metric to appear in the list of available metrics.
- The graph doesn't refresh itself automatically. To update the display, choose the refresh () icon.
- If health checks are failing for some reason, such as a connection timeout, Route 53 can't measure latency, and latency data will be missing from the graph for the affected period.

Monitoring health checks using CloudWatch

Route 53 health checks integrate with CloudWatch metrics so that you can do the following:

- Verify that a health check is properly configured.
- Review the status of a health check over a specified period of time.
- Configure CloudWatch to send an Amazon SNS alert when the status of a health check is unhealthy. Note that several minutes might elapse between the time that a health check fails and the time that you receive the associated SNS notification.

For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

- [To view the status of a health check \(console\) \(p. 533\)](#)
- [To receive an Amazon SNS notification when a health check status is unhealthy \(console\) \(p. 533\)](#)
- [To view CloudWatch alarm status and edit alarms for Amazon Route 53 \(console\) \(p. 536\)](#)
- [To view Route 53 metrics on the CloudWatch console \(p. 536\)](#)

To view the status of a health check (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. Choose the rows for the applicable health checks.
4. In the bottom pane, choose the **Monitoring** tab.

The two graphs display the status for the last hour in one-minute intervals:

Health check status

The graph shows the Route 53 assessment of endpoint health. **1** indicates healthy and **0** indicates unhealthy.

Health checkers that report the endpoint healthy (%)

For health checks that monitor an endpoint only, the graph shows the percentage of Route 53 health checkers that consider the selected endpoint to be healthy.

When a health check is disabled, this metric isn't available.

Number of healthy child health checks

For calculated health checks only, the graph shows the number of child health checks that are healthy.

Note

If you selected more than one health check, the graph displays a separate color-coded line for each health check.

5. To view a larger graph and specify different settings, click the graph. You can change the following settings:

Statistic

Changes the calculation that CloudWatch performs on the data.

Time range

Displays the status of a health check over a different period, for example, overnight or last week.

Period

Changes the interval between data points in the graph.

Note the following:

- If you just created a health check, you might need to wait for a few minutes for data to appear in the graph and for the health check metric to appear in the list of available metrics.
- The graph doesn't refresh itself automatically. To update the display, choose the refresh () icon.

To receive an Amazon SNS notification when a health check status is unhealthy (console)

1. In the navigation pane of the Route 53 console, choose **Health Checks**.
2. Choose the row for the applicable health check.
3. In the bottom pane, choose the **Alarms** tab.

The table lists the alarms that you've already created for this health check.

4. Choose **Create Alarm**.
5. Specify the following values:

Alarm name

Enter the name that you want Route 53 to display in the **Name** column on the **Alarms** tab.

Alarm description

(Optional) Enter a description for the alarm. This value appears in the CloudWatch console.

Send notification

Choose whether you want Route 53 to send you notification if the status of this health check triggers an alarm.

Notification target (Only when "Send notification" is "Yes")

If you want CloudWatch to send notification to an existing SNS topic, choose the topic from the list.

If you want CloudWatch to send notification but not to an existing SNS topic, do one of the following:

- **If you want CloudWatch to send email notification** – Choose **New SNS topic** and continue with this procedure.
- **If you want CloudWatch to send notification by another method** – Open a new browser tab, go to the Amazon SNS console, and create the new topic. Then return to the Route 53 console, choose the name of the new topic from the **Notification target** list, and continue with this procedure.

Topic name (Only when you choose to create a new Amazon SNS topic)

Enter a name for the new Amazon SNS topic.

Recipient email addresses (Only when you choose to create a new Amazon SNS topic)

Enter the email address that you want Route 53 to send an SNS notification to when a health check triggers an alarm.

Alarm target

Choose the value that you want Route 53 to evaluate for this health check:

- **Health check status** – Route 53 health checkers report that the health check is healthy or unhealthy
- **Health checkers that report the endpoint healthy (%)** (health checks that monitor an endpoint only) – The percentage of Route 53 health checkers that report that the status of the health check is healthy
- **Number of healthy child health checks** (calculated health checks only) – The number of child health checks in a calculated health check that report that the status of the health check is healthy
- **TCP connection time** (HTTP and TCP health checks only) – The time in milliseconds that it took Route 53 health checkers to establish a TCP connection with the endpoint
- **Time to complete SSL handshake** (HTTPS health checks only) – The time in milliseconds that it took Route 53 health checkers to complete the SSL/TLS handshake
- **Time to first byte** (HTTP and HTTPS health checks only) – The time in milliseconds that it took Route 53 health checkers to receive the first byte of the response to an HTTP or HTTPS request

Alarm target

For the alarm targets that are based on latency (**TCP connection time**, **Time to complete SSL handshake**, **Time to first byte**), choose whether you want CloudWatch to calculate latency for Route 53 health checkers in a specific region or for all regions (**Global**).

Note that if you choose a region, Route 53 measures latency only twice per minute, and the number of samples will be smaller than if you choose all regions. As a result, outlying values are more likely. To prevent spurious alarm notifications, we recommend that you specify a larger number of consecutive periods that the health check must fail before CloudWatch sends you a notification.

Fulfill condition

Use the following settings to determine when CloudWatch should trigger an alarm.

Alarm target	Recommended condition	Description
Health check status	Minimum < 1	Route 53 health checkers report when the endpoint is unhealthy.
Health checkers that report the endpoint healthy (%)	Average < desired percentage	<i>Health checks that monitor an endpoint only</i> – Route 53 considers the status of a health check to be unhealthy when less than 18% of health checkers report that the status is healthy. Don't choose Sample Count for this metric because the range of sample counts can change as Route 53 adds more health checking regions. Average will always accurately represent the percentage of checkers that are reporting the status of a health check.
Number of healthy child health checks	Minimum < desired number of healthy child health checks	The Minimum statistic returns the most conservative value and represents the worst-case scenario.
TCP connection time	Average > desired time in milliseconds	Average is a more consistent value than other statistics.
Time to complete SSL handshake	Average > desired time in milliseconds	Average is a more consistent value than other statistics.
Time to first byte	Average > desired time in milliseconds	Average is a more consistent value than other statistics.

For at least **x** consecutive periods of **y** minutes/hours/day

Specify how many consecutive time periods that the specified value must meet the criteria before Route 53 sends notification. Then specify the length of the time period.

6. When you choose **Create**, Amazon SNS sends you an email with information about the new SNS topic.
7. In the email, choose **Confirm subscription**. You must confirm your subscription to begin receiving CloudWatch notifications.

To view CloudWatch alarm status and edit alarms for Amazon Route 53 (console)

1. In the navigation pane of the Route 53 console, choose **Health Checks**.
2. Choose the row for any health check.
3. In the details pane (following x **Health Checks Selected**), choose the right caret (>) icon.

The **CloudWatch Alarms** list contains all the Route 53 alarms that you have created using the current AWS account.

The **State** column shows the current status of each alarm:

OK

CloudWatch has accumulated enough statistics from Route 53 health checks to determine that the endpoint doesn't meet the alarm threshold.

INSUFFICIENT DATA

CloudWatch hasn't accumulated enough statistics to determine whether the endpoint meets the alarm threshold. This is the initial state of a new alarm. The alarm state also changes to **INSUFFICIENT DATA** if CloudWatch metrics become unavailable or if you delete the health check without deleting the associated alarm.

ALARM

CloudWatch has accumulated enough statistics from Route 53 health checks to determine that the endpoint meets the alarm threshold and to send notification to the specified email address.

4. To view or edit settings for an alarm, choose the name of the alarm.
5. To view an alarm in the CloudWatch console, which provides more detailed information about the alarm (for example, a history of updates to the alarm and changes in status), choose **View** in the **More Options** column for the alarm.
6. To view all the CloudWatch alarms that you created using the current AWS account, including alarms for other AWS services, choose **View All CloudWatch Alarms**.
7. To view all the available CloudWatch metrics, including metrics that aren't currently being used by the current AWS account, choose **View All CloudWatch Metrics**.

To view Route 53 metrics on the CloudWatch console

1. Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Change the current region to **US East (N. Virginia)**. Route 53 metrics are not available if you select any other region as the current region.
3. In the navigation pane, choose **Metrics**.
4. On the **All metrics** tab, choose **Route 53**.
5. Choose **Health Check Metrics**.

Configuring DNS failover

When you have more than one resource performing the same function—for example, more than one HTTP server or mail server—you can configure Amazon Route 53 to check the health of your resources and respond to DNS queries using only the healthy resources. For example, suppose your website, example.com, is hosted on six servers, two each in three data centers around the world. You can configure Route 53 to check the health of those servers and to respond to DNS queries for example.com using only the servers that are currently healthy.

Route 53 can check the health of your resources in both simple and complex configurations:

- In simple configurations, you create a group of records that all have the same name and type, such as a group of weighted records with a type of A for example.com. You then configure Route 53 to check the health of the corresponding resources. Route 53 responds to DNS queries based on the health of your resources. For more information, see [How health checks work in simple Amazon Route 53 configurations \(p. 538\)](#).
- In more complex configurations, you create a tree of records that route traffic based on multiple criteria. For example, if latency for your users is your most important criterion, then you might use latency alias records to route traffic to the region that provides the best latency. The latency alias records might have weighted records in each region as the alias target. The weighted records might route traffic to EC2 instances based on the instance type. As with a simple configuration, you can configure Route 53 to route traffic based on the health of your resources. For more information, see [How health checks work in complex Amazon Route 53 configurations \(p. 541\)](#).

Topics

- [Task list for configuring DNS failover \(p. 537\)](#)
- [How health checks work in simple Amazon Route 53 configurations \(p. 538\)](#)
- [How health checks work in complex Amazon Route 53 configurations \(p. 541\)](#)
- [How Amazon Route 53 chooses records when health checking is configured \(p. 546\)](#)
- [Active-active and active-passive failover \(p. 547\)](#)
- [Configuring failover in a private hosted zone \(p. 550\)](#)
- [How Amazon Route 53 averts failover problems \(p. 550\)](#)

Task list for configuring DNS failover

To use Route 53 to configure DNS failover, perform the following tasks:

1. Draw a complete tree diagram of your configuration, and indicate which type of record you're creating (weighted alias, failover, latency, and so on) for each node. At the top of the tree put the records for the domain name, such as example.com, that your users will use to access your website or web application.

The kinds of records that appear in your tree diagram depend on the complexity of the configuration:

- In a simple configuration, either your diagram won't include any alias records, or the alias records will route traffic directly to a resource, such as an ELB load balancer, instead of to another Route 53 record. For more information, see [How health checks work in simple Amazon Route 53 configurations \(p. 538\)](#).
- In a complex configuration, your diagram will include a combination of alias records (such as weighted alias and failover alias) and non-alias records in a multi-level tree like the examples in the topic [How health checks work in complex Amazon Route 53 configurations \(p. 541\)](#).

Note

To quickly and easily create records for complex routing configurations and associate the records with health checks, you can use the traffic flow visual editor and save the configuration as a traffic policy. You can then associate the traffic policy with one or more domain names (such as example.com) or subdomain names (such as www.example.com), in the same hosted zone or in multiple hosted zones. In addition, you can roll back the updates if the new configuration isn't performing as you expected it to. For more information, see [Using traffic flow to route DNS traffic \(p. 442\)](#).

For more information, see the following documentation:

- [Choosing a routing policy \(p. 371\)](#)
 - [Choosing between alias and non-alias records \(p. 379\)](#)
2. Create health checks for the resources that you can't create alias records for, such as Amazon EC2 servers and email servers running in your data center. You'll associate these health checks with your non-alias records.

For more information, see [Creating, updating, and deleting health checks \(p. 518\)](#).

3. If necessary, configure router and firewall rules so that Route 53 can send regular requests to the endpoints that you specified in your health checks. For more information, see [Configuring router and firewall rules for Amazon Route 53 health checks \(p. 529\)](#).
4. Create all the non-alias records in your diagram, and associate the health checks that you created in step 2 with the applicable records.

If you're configuring DNS failover in a configuration that doesn't include any alias records, skip the remaining tasks.

5. Create the alias records that route traffic to AWS resources, such as ELB load balancers and CloudFront distributions. If you want Route 53 to try another branch of the tree when a resource is unhealthy, set the value of **Evaluate Target Health** to **Yes** for each of your alias records. (**Evaluate Target Health** isn't supported for some AWS resources.)
6. Starting at the bottom of the tree diagram that you created in step 1, create the alias records that route traffic to the records that you created in steps 4 and 5. If you want Route 53 to try another branch of the tree when all the non-alias records are unhealthy in a branch of your tree, set the value of **Evaluate Target Health** to **Yes** for each of your alias records.

Remember that you can't create an alias record that routes traffic to another record until you have created the other record.

How health checks work in simple Amazon Route 53 configurations

When you have two or more resources that perform the same function, such as two or more web servers for example.com, you can use the following health-checking features to route traffic only to the healthy resources:

Check the health of EC2 instances and other resources (non-alias records)

If you're routing traffic to resources that you can't create alias records for, such as EC2 instances, you create a record and a health check for each resource. Then you associate each health check with the applicable record. Health checks regularly check the health of the corresponding resources, and Route 53 routes traffic only to the resources that health checks report as healthy.

Evaluate the health of an AWS resource (alias records)

If you're using [alias records](#) to route traffic to selected AWS resources, such as ELB load balancers, you can configure Route 53 to evaluate the health of the resource and to route traffic only to resources that are healthy. When you configure an alias record to evaluate the health of a resource, you don't need to create a health check for the resource.

Here's an overview of how you configure Route 53 to check the health of your resources in simple configurations:

1. You identify the resources that you want Route 53 to monitor. For example, you might want to monitor all the HTTP servers that respond to requests for example.com.
2. You create health checks for the resources that you can't create alias records for, such as EC2 instances or servers in your own data center. You specify how to send health-checking requests to the resource: which protocol to use (HTTP, HTTPS, or TCP), which IP address and port to use, and, for HTTP/HTTPS health checks, a domain name and path.

Note

If you're using any resources that you can create alias records for, such as ELB load balancers, don't create health checks for those resources.

A common configuration is to create one health check for each resource and to use the same IP address for the health check endpoint as for the resource. The health check sends requests to the specified IP address.

Note

Route 53 can't check the health of resources that have an IP address in local, private, nonroutable, or multicast ranges. For more information about IP addresses that you can't create health checks for, see [RFC 5735, Special Use IPv4 Addresses](#) and [RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space](#).

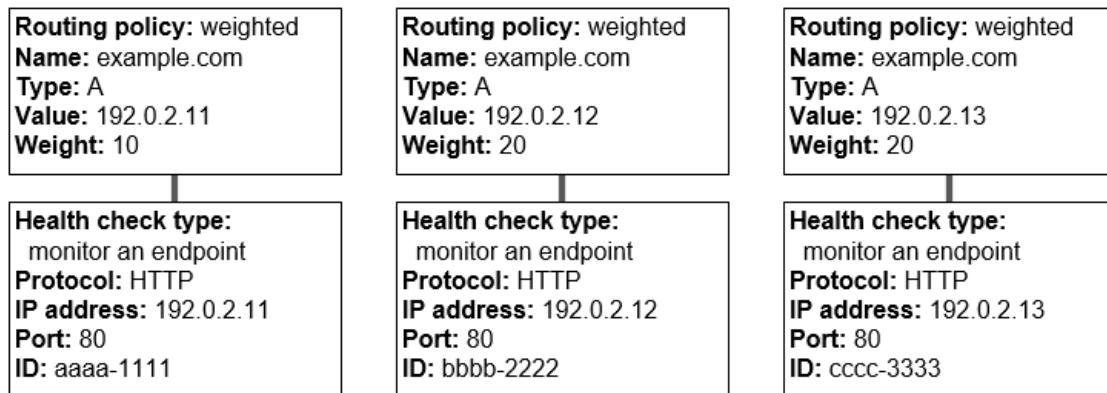
For more information about creating health checks, see [Creating, updating, and deleting health checks \(p. 518\)](#).

3. You might need to configure router and firewall rules so that Route 53 can send regular requests to the endpoints that you specified in your health checks. For more information, see [Configuring router and firewall rules for Amazon Route 53 health checks \(p. 529\)](#).
4. You create a group of records for your resources, for example, a group of weighted records. You can mix alias and non-alias records, but they all must have the same value for **Name**, **Type**, and **Routing Policy**.

How you configure Route 53 to check the health of your resources depends on whether you're creating alias records or non-alias records:

- **Alias records** – Specify **Yes** for **Evaluate Target Health**.
- **Non-alias records** – Associate the health checks that you created in step 2 with the corresponding records.

When you're finished, your configuration looks similar to the following diagram, which includes only non-alias records.



For more information about creating records by using the Route 53 console, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

5. If you created health checks, Route 53 periodically sends requests to the endpoint for each health check; it doesn't perform the health check when it receives a DNS query. Based on the responses, Route 53 decides whether the endpoints are healthy and uses that information to determine how to respond to queries. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

Route 53 doesn't check the health of the resource specified in the record, such as the IP address that is specified in an A record for example.com. When you associate a health check with a record, Route 53 begins to check the health of the endpoint that you specified in the health check. You can also configure Route 53 to monitor the health of other health checks or monitor the data streams for CloudWatch alarms. For more information, see [Types of Amazon Route 53 health checks \(p. 516\)](#).

Here's what happens when Route 53 receives a query for example.com:

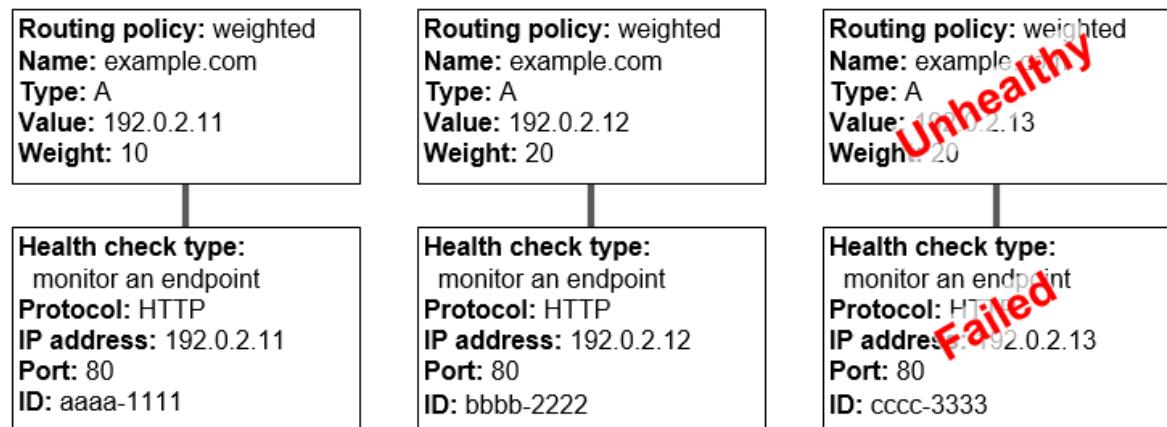
1. Route 53 chooses a record based on the routing policy. In this case, it chooses a record based on weight.
2. It determines the current health of the selected record by checking the status of the health check for that record.
3. If the selected record is unhealthy, Route 53 chooses a different record. This time, the unhealthy record isn't considered.

For more information, see [How Amazon Route 53 chooses records when health checking is configured \(p. 546\)](#).

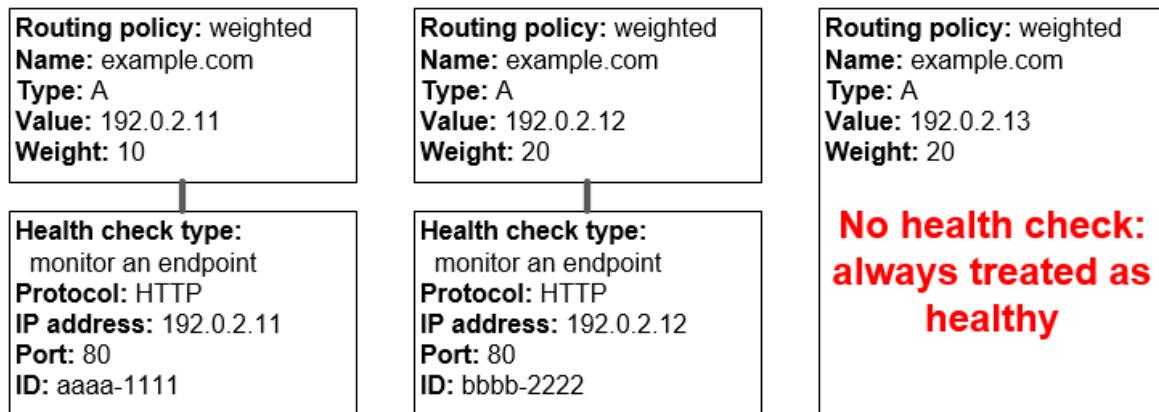
4. When Route 53 finds a healthy record, it responds to the query with the applicable value, such as the IP address in an A record.

The following example shows a group of weighted records in which the third record is unhealthy. Initially, Route 53 selects a record based on the weights of all three records. If it happens to select the unhealthy record the first time, Route 53 selects another record, but this time it omits the weight of the third record from the calculation:

- When Route 53 initially selects from among all three records, it responds to requests using the first record about 20% of the time, $10/(10 + 20 + 20)$.
- When Route 53 determines that the third record is unhealthy, it responds to requests using the first record about 33% of the time, $10/(10 + 20)$.



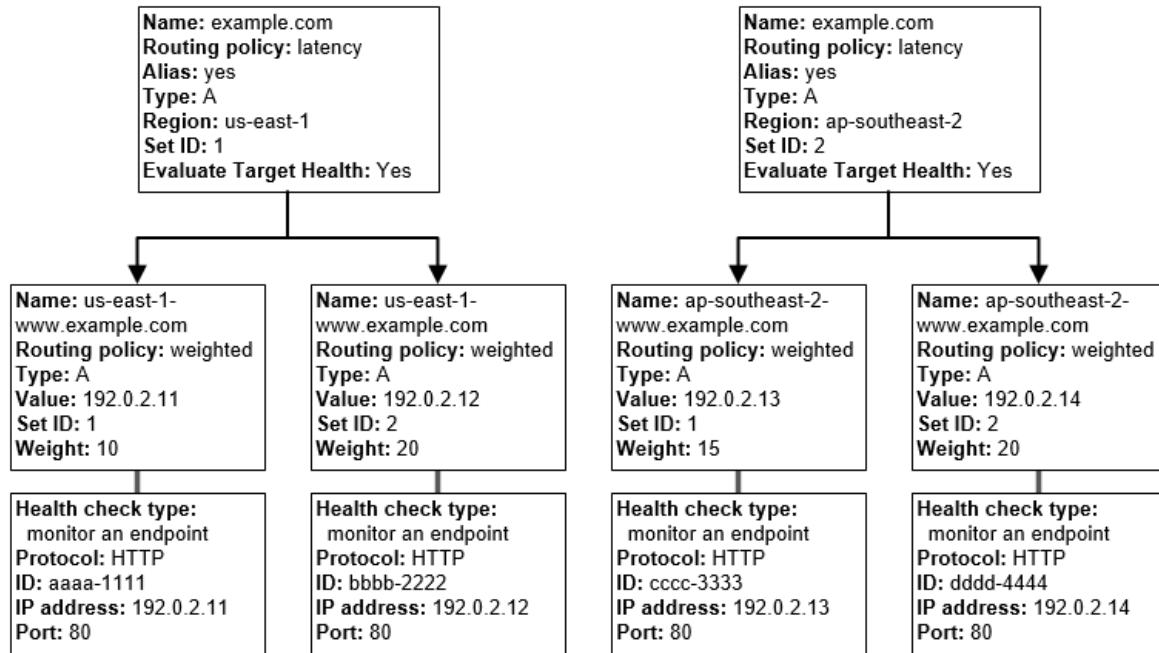
If you omit a health check from one or more records in a group of records, Route 53 has no way to determine the health of the corresponding resource. Route 53 treats those records as healthy.



How health checks work in complex Amazon Route 53 configurations

Checking the health of resources in complex configurations works much the same way as in simple configurations. However, in complex configurations, you use a combination of alias records (such as weighted alias and failover alias) and non-alias records to build a decision tree that gives you greater control over how Route 53 responds to requests.

For example, you might use latency alias records to select a region close to a user and use weighted records for two or more resources within each region to protect against the failure of a single endpoint or an Availability Zone. The following diagram shows this configuration.



Here's how Amazon EC2 and Route 53 are configured. Let's start at the bottom of the tree because that's the order that you'll create records in:

- You have two EC2 instances in each of two regions, us-east-1 and ap-southeast-2. You want Route 53 to route traffic to your EC2 instances based on whether they're healthy, so you create a health

check for each instance. You configure each health check to send health-checking requests to the corresponding instance at the Elastic IP address for the instance.

Route 53 is a global service, so you don't specify the region that you want to create health checks in.

- You want to route traffic to the two instances in each region based on the instance type, so you create a weighted record for each instance and give each record a weight. (You can change the weight later to route more or less traffic to an instance.) You also associate the applicable health check with each instance.

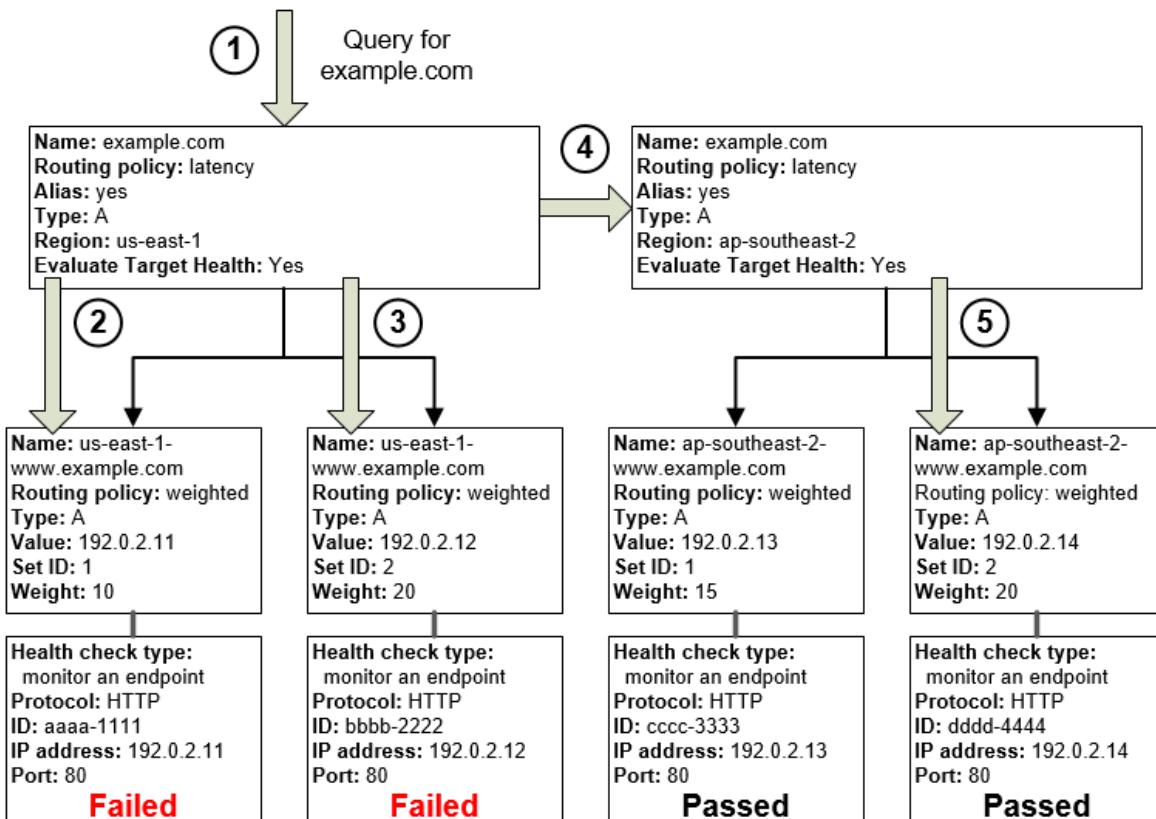
When you create the records, you use names such as us-east-1-www.example.com. and ap-southeast-2-www.example.com. You'll wait until you get to the top of the tree to give records the names that your users will use to access your website or web application, such as example.com.

- You want to route traffic to the region that provides the lowest latency for your users, so you choose the latency [routing policy](#) for the records at the top of the tree.

You want to route traffic to the *records* in each region, not directly to the *resources* in each region (the weighted records already do that). As a result, you create latency [alias records](#).

When you create the alias records, you give them the name that you want your users to use to access your website or web application, such as example.com. The alias records route traffic for example.com to the us-east-1-www.example.com and ap-southeast-2-www.example.com records.

For both latency alias records, you set the value of **Evaluate Target Health** to Yes. This causes Route 53 to determine whether there are any healthy resources in a region before trying to route traffic there. If not, Route 53 chooses a healthy resource in the other region.



The preceding diagram illustrates the following sequence of events:

1. Route 53 receives a query for example.com. Based on the latency for the user making the request, Route 53 selects the latency alias record for the us-east-1 region.
2. Route 53 selects a weighted record based on weight. **Evaluate Target Health** is **Yes** for the latency alias record, so Route 53 checks the health of the selected weighted record.
3. The health check failed, so Route 53 chooses another weighted record based on weight and checks its health. That record also is unhealthy.
4. Route 53 backs out of that branch of the tree, looks for the latency alias record with the next-best latency, and chooses the record for ap-southeast-2.
5. Route 53 again selects a record based on weight, and then checks the health of the selected resource. The resource is healthy, so Route 53 returns the applicable value in response to the query.

Topics

- [What happens when you associate a health check with an alias record? \(p. 543\)](#)
- [What happens when you omit health checks? \(p. 544\)](#)
- [What happens when you set evaluate target health to No? \(p. 545\)](#)

What happens when you associate a health check with an alias record?

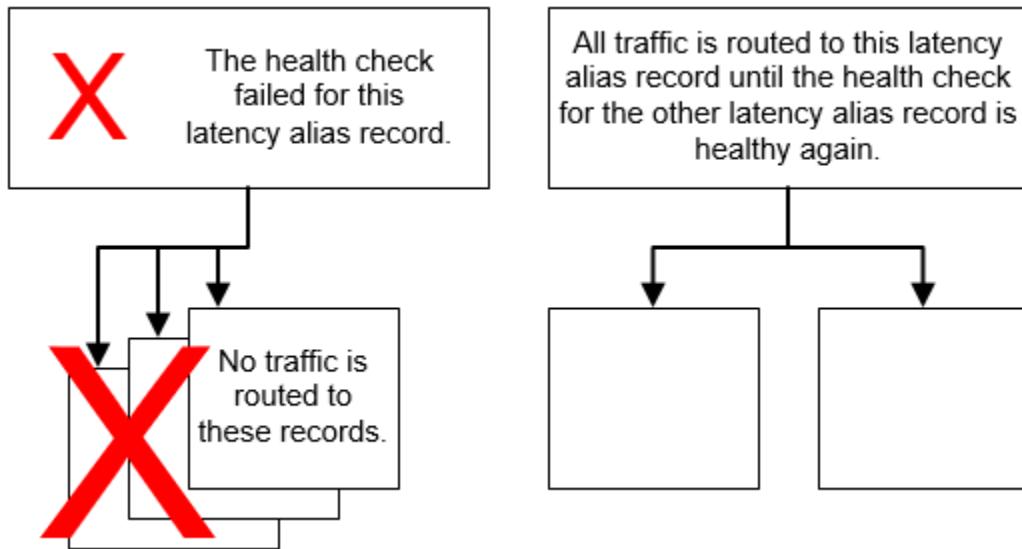
You can associate a health check with an alias record instead of or in addition to setting the value of **Evaluate Target Health** to **Yes**. However, it's generally more useful if Route 53 responds to queries based on the health of the underlying resources—the HTTP servers, database servers, and other resources that your alias records refer to. For example, suppose the following configuration:

- You assign a health check to a latency alias record for which the alias target is a group of weighted records.
- You set the value of **Evaluate Target Health** to **Yes** for the latency alias record.

In this configuration, both of the following must be true before Route 53 will return the applicable value for a weighted record:

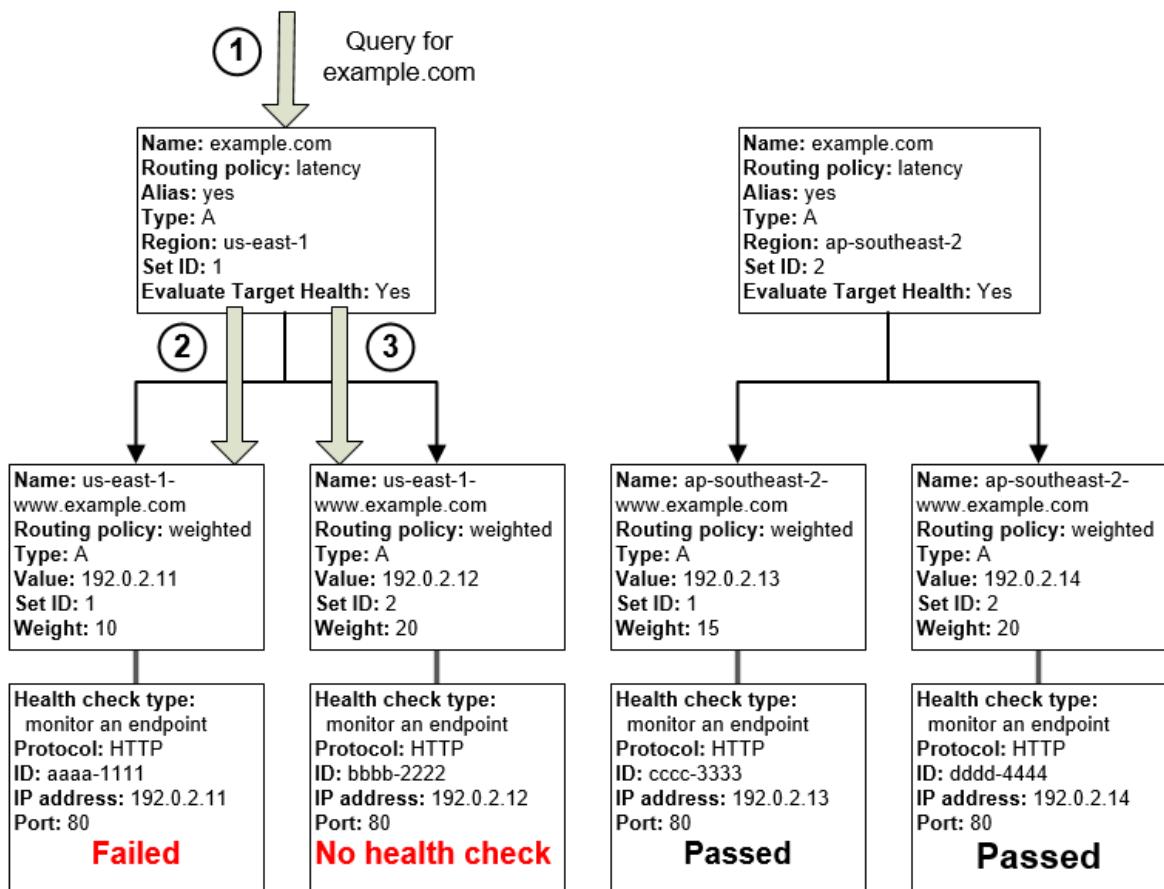
- The health check associated with the latency alias record must pass.
- At least one weighted record must be considered healthy, either because it's associated with a health check that passes or because it's not associated with a health check. In the latter case, Route 53 always considers the weighted record healthy.

In the following illustration, the health check for the latency alias record on the top left failed. As a result, Route 53 stops responding to queries using any of the weighted records that the latency alias record refers to even if they're all healthy. Route 53 begins to consider these weighted records again only when the health check for the latency alias record is healthy again. (For exceptions, see [How Amazon Route 53 chooses records when health checking is configured \(p. 546\)](#).)



What happens when you omit health checks?

In a complex configuration, it's important to associate health checks with all the non-alias records. In the following example, a health check is missing on one of the weighted records in the us-east-1 region.



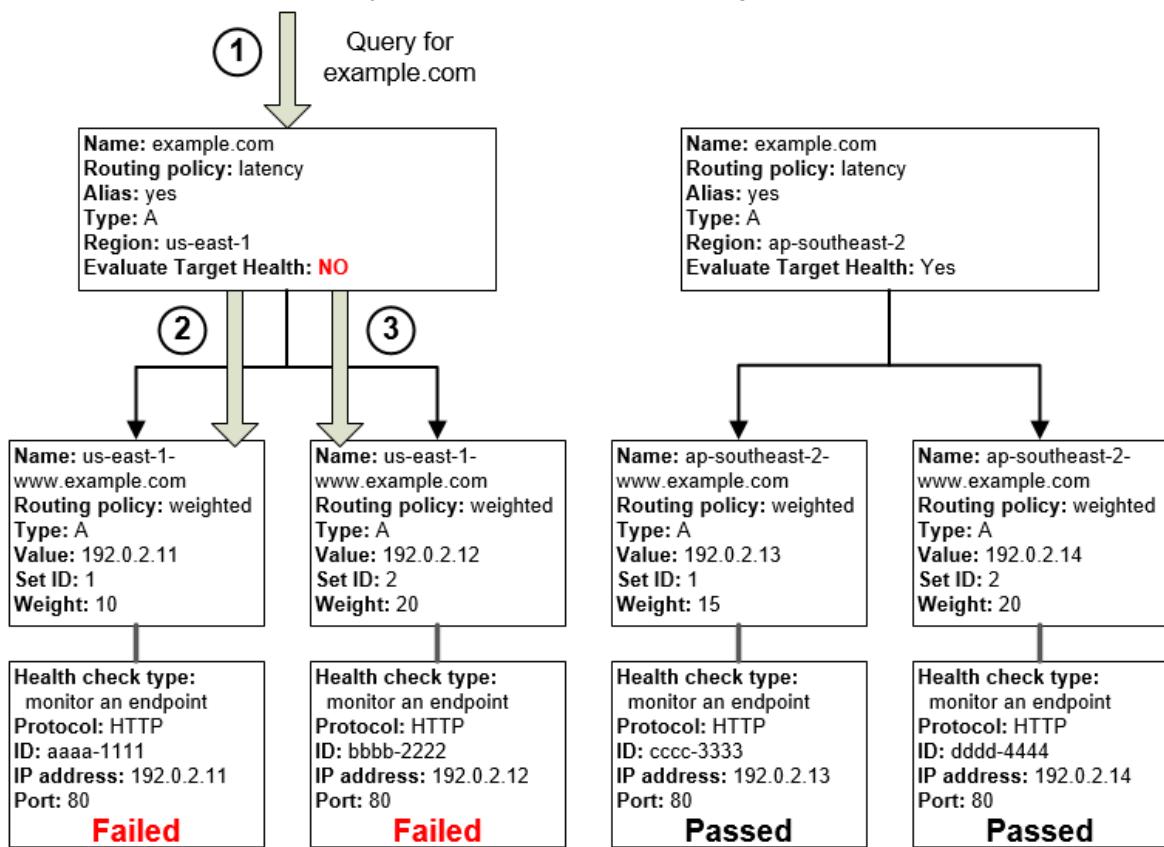
Here's what happens when you omit a health check on a non-alias record in this configuration:

1. Route 53 receives a query for example.com. Based on the latency for the user making the request, Route 53 selects the latency alias record for the us-east-1 region.
2. Route 53 looks up the alias target for the latency alias record, and checks the status of the corresponding health checks. The health check for one weighted record failed, so that record is omitted from consideration.
3. The other weighted record in the alias target for the us-east-1 region has no health check. The corresponding resource might or might not be healthy, but without a health check, Route 53 has no way to know. Route 53 assumes that the resource is healthy and returns the applicable value in response to the query.

What happens when you set evaluate target health to No?

In general, you should set **Evaluate Target Health** to **Yes** for all the alias records in a tree. If you set **Evaluate Target Health** to **No**, Route 53 continues to route traffic to the records that an alias record refers to even if health checks for those records are failing.

In the following example, all the weighted records have associated health checks, but **Evaluate Target Health** is set to **No** for the latency alias record for the us-east-1 region:



Here's what happens when you set **Evaluate Target Health** to **No** for an alias record in this configuration:

1. Route 53 receives a query for example.com. Based on the latency for the user making the request, Route 53 selects the latency alias record for the us-east-1 region.
2. Route 53 determines what the alias target is for the latency alias record, and checks the corresponding health checks. They're both failing.

3. Because the value of **Evaluate Target Health** is **No** for the latency alias record for the us-east-1 region, Route 53 must choose one record in this branch instead of backing out of the branch and looking for a healthy record in the ap-southeast-2 region.

How Amazon Route 53 chooses records when health checking is configured

If you configure health checking for all the records in a group of records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or failover), Route 53 responds to DNS queries by choosing a healthy record and returning the applicable value from that record.

For example, suppose you create three weighted A records, and you assign health checks to all three. If the health check for one of the records is unhealthy, Route 53 responds to DNS queries with the IP addresses in one of the other two records.

Here's how Route 53 chooses a healthy record:

1. Route 53 initially chooses a record based on the routing policy and on the values that you specify for each record. For example, for weighted records, Route 53 chooses a record based on the weight that you specify for each record.
2. Route 53 determines whether the record is healthy:
 - **Non-alias record with an associated health check** – If you associated a health check with a non-alias record, Route 53 checks the current status of the health check.

Route 53 periodically checks the health of the endpoint that is specified in a health check; it doesn't perform the health check when the DNS query arrives.

You can associate health checks with alias records, but we recommend that you associate health checks only with non-alias records. For more information, see [What happens when you associate a health check with an alias record? \(p. 543\)](#).

- **Alias record with Evaluate Target Health set to Yes** – Route 53 checks the health status of the resource that the alias record references, for example, an ELB load balancer or another record in the same hosted zone.
3. If the record is healthy, Route 53 responds to the query with the applicable value, such as an IP address.

If the record is unhealthy, Route 53 chooses another record using the same criteria and repeats the process until it finds a healthy record.

Route 53 uses the following criteria when choosing a record:

Records without a health check are always healthy

If a record in a group of records that have the same name and type doesn't have an associated health check, Route 53 always considers it healthy and always includes it among possible responses to a query.

If no record is healthy, all records are healthy

If none of the records in a group of records are healthy, Route 53 needs to return something in response to DNS queries, but it has no basis for choosing one record over another. In this circumstance, Route 53 considers all the records in the group to be healthy and selects one based on the routing policy and on the values that you specify for each record.

Weighted records that have a weight of 0

If you add health checks to all the records in a group of weighted records, but you give nonzero weights to some records and zero weights to others, health checks work the same as when all records have nonzero weights with the following exceptions:

- Route 53 initially considers only the nonzero weighted records, if any.
- If all the records that have a weight greater than 0 are unhealthy, then Route 53 considers the zero-weighted records.

For more information about weighted records, see [Weighted routing \(p. 378\)](#).

Alias records

You can also configure health checking for alias records by setting **Evaluate Target Health** to **Yes** for each alias record. This causes Route 53 to evaluate the health of the resource that the record routes traffic to, for example, an ELB load balancer or another record in the same hosted zone.

For example, suppose the alias target for an alias record is a group of weighted records that all have nonzero weights:

- As long as at least one of the weighted records is healthy, Route 53 considers the alias record to be healthy.
- If none of the weighted records is healthy, Route 53 considers the alias record to be unhealthy.
- Route 53 stops considering records in that branch of the tree until at least one weighted record becomes healthy again.

For more information, see [How health checks work in complex Amazon Route 53 configurations \(p. 541\)](#).

Failover records

Failover records generally work the same way as other routing types. You create health checks and associate them with non-alias records, and you set **Evaluate Target Health** to **Yes** for alias records. Note the following:

- Both the primary and secondary records can be a non-alias record or an alias record.
- If you associate health checks with both the primary and secondary failover records, here's how Route 53 responds to requests:
 - If Route 53 considers the primary record healthy (if the health check endpoint is healthy), Route 53 returns only the primary record in response to a DNS query.
 - If Route 53 considers the primary record unhealthy and the secondary record healthy, Route 53 returns the secondary record instead.
 - If Route 53 considers both the primary and secondary records unhealthy, Route 53 returns the primary record.
- When you're configuring the secondary record, adding a health check is optional. If you omit the health check for the secondary record, and if the health check endpoint for the primary record is unhealthy, Route 53 always responds to DNS queries by using the secondary record. This is true even if the secondary record is unhealthy.

For more information, see the following topics:

- [Configuring active-passive failover with one primary and one secondary resource \(p. 548\)](#)
- [Configuring active-passive failover with multiple primary and secondary resources \(p. 548\)](#)

Active-active and active-passive failover

You can use Route 53 health checking to configure active-active and active-passive failover configurations. You configure active-active failover using any [routing policy](#) (or combination of routing policies) other than failover, and you configure active-passive failover using the failover routing policy.

Topics

- [Active-active failover \(p. 548\)](#)
- [Active-passive failover \(p. 548\)](#)

Active-active failover

Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.

Active-passive failover

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

Topics

- [Configuring active-passive failover with one primary and one secondary resource \(p. 548\)](#)
- [Configuring active-passive failover with multiple primary and secondary resources \(p. 548\)](#)
- [Configuring active-passive failover with weighted records \(p. 549\)](#)

Configuring active-passive failover with one primary and one secondary resource

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify **Failover** for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route 53 responds to DNS queries using the secondary record.

Configuring active-passive failover with multiple primary and secondary resources

You can also associate multiple resources with the primary record, the secondary record, or both. In this configuration, Route 53 considers the primary failover record to be healthy as long as at least one of the associated resources is healthy. For more information, see [How Amazon Route 53 chooses records when health checking is configured \(p. 546\)](#).

To configure active-passive failover with multiple resources for the primary or secondary record, perform the following tasks.

1. Create a health check for each resource that you want to route traffic to, such as an EC2 instance or a web server in your data center.

Note

If you're routing traffic to any AWS resources that you can create [alias records](#) for, don't create health checks for those resources. When you create the alias records, you set **Evaluate Target Health** to **Yes** instead.

For more information, see [Creating and updating health checks \(p. 519\)](#).

2. Create records for your primary resources, and specify the following values:

- Give each record the same name, type, and routing policy. For example, you might create three weighted A records that are all named failover-primary.example.com.
- If you're using AWS resources that you can create alias records for, specify **Yes** for **Evaluate Target Health**.

If you're using resources that you can't create alias records for, associate the applicable health check from step 1 with each record.

For more information, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

3. Create records for your secondary resources, if applicable, and specify the following values:

- Give each record the same name, type, and routing policy. For example, you might create three weighted A records that are all named failover-secondary.example.com.
- If you're using AWS resources that you can create alias records for, specify **Yes** for **Evaluate Target Health**.

If you're using resources that you can't create alias records for, associate the applicable health check from step 1 with each record.

Note

Some customers use a web server as their primary resource and an Amazon S3 bucket that is configured as a website endpoint as their secondary resource. The S3 bucket contains a simple "temporarily unavailable" message. If you're using that configuration, you can skip this step and just create a failover alias record for the secondary resource in step 4.

4. Create two failover alias records, one primary and one secondary, and specify the following values:

Primary record

- **Name** – Specify the domain name (example.com) or the subdomain name (www.example.com) that you want Route 53 to route traffic for.
- **Alias** – Specify **Yes**.
- **Alias Target** – Specify the name of the records that you created in step 2.
- **Routing Policy** – Specify **Failover**.
- **Failover Record Type** – Specify **Primary**.
- **Evaluate Target Health** – Specify **Yes**.
- **Associate with Health Check** – Specify **No**.

Secondary record

- **Name** – Specify the same name that you specified for the primary record.
- **Alias** – Specify **Yes**.
- **Alias Target** – If you created records for your secondary resource in step 3, specify the name of the records. If you're using an Amazon S3 bucket for the secondary resource, specify the DNS name of the website endpoint.
- **Routing Policy** – Specify **Failover**.
- **Failover Record Type** – Specify **Secondary**.
- **Evaluate Target Health** – Specify **Yes**.
- **Associate with Health Check** – Specify **No**.

Configuring active-passive failover with weighted records

You can also use weighted records for active-passive failover, with caveats. If you specify nonzero weights for some records and zero weights for other records, Route 53 responds to DNS queries using API Version 2013-04-01. 549

only healthy records that have nonzero weights. If all the records that have a weight greater than 0 are unhealthy, then Route 53 responds to queries using the zero-weighted records.

Note

All the records with nonzero weights must be unhealthy before Route 53 starts to respond to DNS queries using records that have weights of zero. This can make your web application or website unreliable if the last healthy resource, such as a web server, can't handle all the traffic when other resources are unavailable.

Configuring failover in a private hosted zone

If you're creating failover records in a private hosted zone, note the following:

- Route 53 health checkers are outside the VPC. To check the health of an endpoint within a VPC by IP address, you must assign a public IP address to the instance in the VPC.
- You can create a CloudWatch metric, associate an alarm with the metric, and then create a health check that is based on the data stream for the alarm. For example, you might create a CloudWatch metric that checks the status of the EC2 StatusCheckFailed metric, add an alarm to the metric, and then create a health check that is based on the data stream for the alarm to check instances within a Virtual Private Cloud (VPC) that only have private IP addresses. For information about creating CloudWatch metrics and alarms by using the CloudWatch console, see the [Amazon CloudWatch User Guide](#).

For more information, see [Working with private hosted zones \(p. 356\)](#).

How Amazon Route 53 averts failover problems

The failover algorithms implemented by Route 53 are designed not only to route traffic to endpoints that are healthy, but also to avoid making disaster scenarios worse due to misconfigured health checks and applications, endpoint overloads, and partition failures.

Topics

- [How Amazon Route 53 averts cascading failures \(p. 550\)](#)
- [How Amazon Route 53 handles internet partitions \(p. 550\)](#)

How Amazon Route 53 averts cascading failures

As a first defense against cascading failures, each request routing algorithm (such as weighted and failover) has a mode of last resort. In this special mode, when all records are considered unhealthy, the Route 53 algorithm reverts to considering all records healthy.

For example, if all instances of an application, on several hosts, are rejecting health check requests, Route 53 DNS servers will choose an answer anyway and return it rather than returning no DNS answer or returning an NXDOMAIN (non-existent domain) response. An application can respond to users but still fail health checks, so this provides some protection against misconfiguration.

Similarly, if an application is overloaded, and one out of three endpoints fails its health checks, so that it's excluded from Route 53 DNS responses, Route 53 distributes responses between the two remaining endpoints. If the remaining endpoints are unable to handle the additional load and they fail, Route 53 reverts to distributing requests to all three endpoints.

How Amazon Route 53 handles internet partitions

Although uncommon, there occasionally are significant internet partitions, meaning that large geographic regions can't communicate with one another over the internet. During these partitions,

Route 53 locations might reach different conclusions about the health status of an endpoint and might differ from the status reported to CloudWatch. Route 53 health checkers in each AWS Region are constantly sending health check statuses to all Route 53 locations. During internet partitions, each Route 53 location might have access only to a partial set of these statuses, usually from its closest regions.

For example, during an internet partition that affects connectivity to and from South America, the Route 53 DNS servers in the Route 53 South America (São Paulo) location might have good access to the health check endpoints in the South America (São Paulo) AWS Region, but poor access to endpoints elsewhere. At the same time, Route 53 in US East (Ohio) might have poor access to health check endpoints in the South America (São Paulo) Region, and conclude that the corresponding records are unhealthy.

Partitions such as these can give rise to situations where Route 53 locations make different conclusions about the health status of endpoints, based on their local visibility of those endpoints. This is why each Route 53 location considers an endpoint healthy when only a portion of reachable health checkers consider it healthy.

Naming and tagging health checks

You can add tags to Amazon Route 53 health checks, which lets you give each health check a name that is more comprehensible than the health check ID. These are the same tags that AWS Billing and Cost Management provides for organizing your AWS bill. For more information about using tags for cost allocation, see [Use cost allocation tags for custom billing reports](#) in the *AWS Billing and Cost Management User Guide*.

Each tag consists of a key (the name of the tag) and a value, both of which you define. When you add tags to a health check, we recommend that you add one tag that has the following values for the key and value:

- **key – Name**
- **value –** The name that you want to give to the health check

The value of the **Name** tag appears in the list of health checks on the Route 53 console, which lets you readily distinguish health checks from one another. To see other tags for a health check, you choose the health check and then choose the **Tags** tab.

For more information about tags, see the following topics:

- To add, edit, or delete the **Name** tag when you add or edit health checks in the Route 53 console, see [Creating, updating, and deleting health checks \(p. 518\)](#).
- For an overview of tagging Route 53 resources, see [Tagging Amazon Route 53 resources \(p. 655\)](#).

Tag restrictions

The following basic restrictions apply to tags:

- Maximum number of tags per resource – 50
- Maximum **Key** length – 128 Unicode characters
- Maximum **Value** length – 256 Unicode characters
- Valid values for **Key** and **Value** – uppercase and lowercase letters in the UTF-8 character set, numbers, space, and the following characters: _ . : / = + - and @
- Tag keys and values are case sensitive

- Don't use the `aws:` prefix for either keys or values; it's reserved for AWS use

Adding, editing, and deleting tags for health checks

The following procedures show you how to use tags for your health checks on the Route 53 console.

Topics

- [To add tags to health checks \(console\) \(p. 552\)](#)
- [To edit tags for health checks \(console\) \(p. 552\)](#)
- [To delete tags for health checks \(console\) \(p. 552\)](#)

To add tags to health checks (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. Select a health check, or select multiple health checks if you want to add the same tag to more than one health check.
4. In the bottom pane, choose the **Tags** tab, and then choose **Add/Edit Tags**.
5. In the **Add/Edit Tags** dialog box, enter a name for the tag in the **Key** field, and enter a value in the **Value** field.
6. Choose **Apply changes**.

To edit tags for health checks (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. Select a health check.

If you select multiple health checks that share the same tag, you cannot edit the value for all the tags simultaneously. Note, however, that you can edit the value of a tag that appears in multiple health checks if you select health checks that have the tag and at least one than doesn't.

For example, suppose you select multiple health checks that have a **Cost Center** tag and one that doesn't. You choose the option to add a tag, and you specify **Cost Center** for the key and **777** for the value. For the selected health checks that already have a **Cost Center** tag, Route 53 changes the value to **777**. For the one health check that doesn't have a **Cost Center** tag, Route 53 adds one and sets the value to **777**.

4. In the bottom pane, choose the **Tags** tab, and then choose **Add/Edit Tags**.
5. In the **Add/Edit Tags** dialog box, edit the value.
6. Choose **Save**.

To delete tags for health checks (console)

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Health Checks**.
3. Select a health check, or select multiple health checks if you want to delete the same tag from more than one health check.

4. In the bottom pane, choose the **Tags** tab, and then choose **Add/Edit Tags**.
5. In the **Add/Edit Tags** dialog box, choose the **X** next to the tag that you want to delete.
6. Choose **Save**.

Using health checks with Amazon Route 53 API versions earlier than 2012-12-12

Health checks are supported starting with the 2012-12-12 version of the Amazon Route 53 API. If a hosted zone contains records that health checks are configured for, we recommend that you use only the 2012-12-12 API or later. Note the following restrictions on using health checks with earlier API versions.

- The `ChangeResourceRecordSets` action cannot create or delete records that include the `EvaluateTargetHealth`, `Failover`, or `HealthCheckId` elements.
- The `ListResourceRecordSets` action can list records that include these elements, but the elements are not included in the output. Instead, the `Value` element of the response contains a message that says the record includes an unsupported attribute.

Route 53 Resolver DNS Firewall

With Route 53 Resolver DNS Firewall, you can filter and regulate outbound DNS traffic for your virtual private cloud (VPC). To do this, you create reusable collections of filtering rules in DNS Firewall rule groups, associate the rule groups to your VPC, and then monitor activity in DNS Firewall logs and metrics. Based on the activity, you can adjust the behavior of DNS Firewall accordingly.

DNS Firewall provides protection for outbound DNS requests from your VPCs. These requests route through Resolver for domain name resolution. A primary use of DNS Firewall protections is to help prevent DNS exfiltration of your data. DNS exfiltration can happen when a bad actor compromises an application instance in your VPC and then uses DNS lookup to send data out of the VPC to a domain that they control. With DNS Firewall, you can monitor and control the domains that your applications can query. You can deny access to the domains that you know to be bad and allow all other queries to pass through. Alternately, you can deny access to all domains except for the ones that you explicitly trust.

You can also use DNS Firewall to block resolution requests to resources in private hosted zones (shared or local) including VPC endpoint names. It can also block requests for public or private Amazon EC2 instance names.

DNS Firewall is a feature of Route 53 Resolver and doesn't require any additional Resolver setup to use.

AWS Firewall Manager supports DNS Firewall

You can use Firewall Manager to centrally configure and manage your DNS Firewall rule group associations for your VPCs across your accounts in AWS Organizations. Firewall Manager automatically adds associations for VPCs that come into scope of your Firewall Manager DNS Firewall policy. For more information, see [AWS Firewall Manager](#) in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

How DNS Firewall works with AWS Network Firewall

DNS Firewall and Network Firewall both offer domain name filtering, but for different types of traffic. With DNS Firewall and Network Firewall together, you can configure domain-based filtering for application layer traffic over two different network paths.

- DNS Firewall provides filtering for outbound DNS queries that pass through the Route 53 Resolver from applications within your VPCs. You can also configure DNS Firewall to send custom responses for queries to blocked domain names.
- Network Firewall provides filtering for both network and application layer traffic, but does not have visibility into queries made by Route 53 Resolver.

For more information about Network Firewall, see the [Network Firewall Developer Guide](#).

How Route 53 Resolver DNS Firewall works

Route 53 Resolver DNS Firewall lets you control access to sites and block DNS-level threats for DNS queries going out from your VPC through the Route 53 Resolver. With DNS Firewall, you define domain name filtering rules in rule groups that you associate with your VPCs. You can specify lists of domain names to allow or block, and you can customize the responses for the DNS queries that you block.

DNS Firewall only filters on the domain name. It does not resolve that name to an IP address to be blocked. Additionally, DNS Firewall filters DNS/UDP traffic, but it doesn't filter other application layer protocols, such as HTTPS, SSH, TLS, FTP, and so on.

Route 53 Resolver DNS Firewall components and settings

You manage DNS Firewall with the following central components and settings.

DNS Firewall rule group

Defines a named, reusable collection of DNS Firewall rules for filtering DNS queries. You populate the rule group with the filtering rules, then associate the rule group with one or more VPCs. When you associate a rule group with a VPC, you enable DNS Firewall filtering for the VPC. Then, when Resolver receives a DNS query for a VPC that has a rule group associated with it, Resolver passes the query to DNS Firewall for filtering.

If you associate multiple rule groups with a single VPC, you indicate their processing order through the priority setting in each association. DNS Firewall processes rule groups for a VPC from the lowest numeric priority setting on up.

For more information, see [DNS Firewall rule groups and rules \(p. 560\)](#).

DNS Firewall rule

Defines a filtering rule for DNS queries in a DNS Firewall rule group. Each rule specifies one domain list and an action to take on DNS queries whose domains match the domain specifications in the list. You can allow, block, or alert on matching queries. You can also define custom responses for blocked queries.

Each rule in a rule group has a priority setting that's unique within the rule group. DNS Firewall processes the rules in a rule group from the lowest numeric priority setting on up.

DNS Firewall rules exist only in the context of the rule group in which they're defined. You can't reuse a rule or reference it independent of its rule group.

For more information, see [DNS Firewall rule groups and rules \(p. 560\)](#).

Domain list

Defines a named, reusable collection of domain specifications for use in DNS filtering. Each rule in a rule group requires a single domain list. You might choose to specify the domains that you want to allow access to, the domains that you want to deny access to, or a combination of both. You can create your own domain lists and you can use domain lists that AWS manages for you.

For more information, see [Route 53 Resolver DNS Firewall domain lists \(p. 563\)](#).

Association between a DNS Firewall rule group and a VPC

Defines a protection for a VPC using a DNS Firewall rule group and enables the Resolver DNS Firewall configuration for the VPC.

If you associate multiple rule groups with a single VPC, you indicate their processing order through the priority setting in the associations. DNS Firewall processes rule groups for a VPC from the lowest numeric priority setting on up.

For more information, see [Enabling Route 53 Resolver DNS Firewall protections for your VPC \(p. 570\)](#).

Resolver DNS Firewall configuration for a VPC

Specifies how Resolver should handle DNS Firewall protections at the VPC level. This configuration is in effect whenever you have at least one DNS Firewall rule group associated with the VPC.

This configuration specifies how Route 53 Resolver handles queries when DNS Firewall fails to filter them. By default, if Resolver doesn't receive a response from DNS Firewall for a query, it fails closed and blocks the query.

For more information, see [DNS Firewall VPC configuration \(p. 571\)](#).

How Route 53 Resolver DNS Firewall filters DNS queries

When a DNS Firewall rule group is associated with your VPC's Route 53 Resolver, the following traffic is filtered by the firewall:

- DNS queries originating within that VPC.
- DNS queries that pass through Resolver endpoints from on-premises resources into that same VPC that has DNS Firewall associated to its resolver.

When DNS Firewall receives a DNS query, it filters the query using the rule groups, rules, and other settings that you've configured and sends the results back to Resolver:

- DNS Firewall evaluates the DNS query using the rule groups that are associated with the VPC until it finds a match or exhausts all of the rule groups. DNS Firewall evaluates the rule groups in order of the priority that you set in the association, starting with the lowest numeric setting. For more information, see [DNS Firewall rule groups and rules \(p. 560\)](#) and [Enabling Route 53 Resolver DNS Firewall protections for your VPC \(p. 570\)](#).
- Within each rule group, DNS Firewall evaluates the DNS query against each rule's domain list until it finds a match or exhausts all rules. DNS Firewall evaluates the rules in order of priority, starting with the lowest numeric setting. For more information, see [DNS Firewall rule groups and rules \(p. 560\)](#).
- When DNS Firewall finds a match with a rule's domain list, it terminates the query evaluation and responds to Resolver with the result. If the action is alert, DNS Firewall also sends an alert to the configured Resolver logs. For more information, see [Rule actions in DNS Firewall \(p. 561\)](#) and [Route 53 Resolver DNS Firewall domain lists \(p. 563\)](#).
- If DNS Firewall evaluates all rule groups without finding a match, it responds to the query as normal.

Resolver routes the query according to the response from DNS Firewall. In the unlikely event that DNS Firewall fails to respond, Resolver applies the VPC's configured DNS Firewall fail mode. For more information, see [DNS Firewall VPC configuration \(p. 571\)](#).

High-level steps for using Route 53 Resolver DNS Firewall

To implement Route 53 Resolver DNS Firewall filtering in your Amazon Virtual Private Cloud VPC, you perform the following high-level steps.

- **Define your filtering approach and your domain lists** – Decide how you want to filter queries, identify the domain specifications that you'll need, and define the logic you'll use to evaluate queries. For example, you might want to allow all queries except for those that are in a list of known bad domains. Or you might want to do the opposite and block all but an approved list of domains, in what is known

as a walled garden approach. You can create and manage your own lists of approved or blocked domain specifications and you can use domain lists that AWS manages for you. For information about domain lists, see [Route 53 Resolver DNS Firewall domain lists \(p. 563\)](#).

- **Create a firewall rule group** – In DNS Firewall, create a rule group to filter DNS queries for your VPC. You must create a rule group in each Region where you want to use it. You might also want to separate your filtering behavior into more than one rule group for reusability in multiple filtering scenarios for your different VPCs. For information about rule groups, see [DNS Firewall rule groups and rules \(p. 560\)](#).
- **Add and configure your rules** – Add a rule to your rule group for each domain list and filtering behavior that you want the rule group to provide. Set the priority settings for your rules so they process in the correct order within the rule group, giving the lowest priority to the rule that you want to evaluate first. For information about rules, see [DNS Firewall rule groups and rules \(p. 560\)](#).
- **Associate the rule group to your VPC** – To begin using your DNS Firewall rule group, associate it with your VPC. If you are using more than one rule group for your VPC, set the priority of each association so the rule groups are processed in the correct order, giving the lowest priority to the rule group that you want to evaluate first. For more information, see [Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group \(p. 570\)](#).
- **(Optional) Change the firewall configuration for the VPC** – If you want Route 53 Resolver to block queries when DNS Firewall fails to send a response back for them, in Resolver, change the VPC's DNS Firewall configuration. For more information, see [DNS Firewall VPC configuration \(p. 571\)](#).

Using Route 53 Resolver DNS Firewall rule groups in multiple Regions

Route 53 Resolver DNS Firewall is a Regional service, so objects that you create in one AWS Region are available only in that Region. To use the same rule group in more than one Region, you must create it in each Region.

The AWS account that created a rule group can share it with other AWS accounts. For more information, see [Sharing Route 53 Resolver DNS Firewall rule groups between AWS accounts \(p. 568\)](#).

Getting started with Route 53 Resolver DNS Firewall

The DNS Firewall console includes a wizard that guides you through the following steps for getting started with DNS Firewall:

- Create rule groups for each set of rules that you want to use.
- For each rule, populate the domain list that you want to inspect for. You can create your own domain lists and you can use AWS managed domain lists.
- Associate your rule groups with the VPCs where you want to use them.

Route 53 Resolver DNS Firewall walled garden example

In this tutorial, you'll create a rule group that blocks all but a select group of domains that you trust. This is called a closed platform, or walled garden approach.

To configure a DNS Firewall rule group using the console wizard

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

- OR -

Sign in to the AWS Management Console and open the the Amazon VPC console under <https://console.aws.amazon.com/vpc/>.
 2. In the navigation pane, choose **Rule groups**.
 3. On the navigation bar, choose the Region for the rule group.
 4. In the **Rule groups** page, choose **Add rule group**.
 5. For the rule group name, enter **WalledGardenExample**. If you want an additional description, enter that as well.
 6. Choose **Next**.
 7. On the **Add rules** page, choose **Add rule**.
 - a. In the **Rule details** pane, enter the rule name **BlockAll**.
 - b. In the **Domain list** pane, select **Add my own domain list**.
 - c. Under **Choose or create a new domain list** select **Create new domain list**.
 - d. Enter a domain list name **AllDomains**, then in the text box, enter an asterisk: *.
 - e. For the action, select **BLOCK** and then leave the response to send at the default setting of **NODATA**.
 - f. Choose **Add rule**. The wizard displays the rule group's **Add rules** page with your **BlockAll** rule listed.
 8. Choose **Add rule** again to add a second rule to your rule group.
 - a. In the **Rule details** pane, enter the rule name **AllowSelectDomains** and leave the description empty.
 - b. In the **Domain list** pane, select **Add my own domain list**.
 - c. Under **Choose or create a new domain list**, select **Create new domain list**.
 - d. Enter a domain list name **ExampleDomains**.
 - e. In the text box, on the first line, enter **example.com** and on the second line, enter **example.org**.
 9. Choose **Next**.
 10. In the **Set rule priority** page, you can adjust the evaluation order of the rules in your rule group. DNS Firewall evaluates rules starting with the lowest priority setting, so the rule at the top of the list is the first one evaluated. For this example, we want DNS Firewall to first identify and allow DNS queries for the select list of domains, and then block any remaining queries.
- Select and adjust the rule ordering so that **AllowSelectDomains** is listed first.
11. Choose **Next**.
 12. In the **Add tags** page, choose **Next**. Tags help you organize and manage your AWS resources. For more information, see [Tagging Amazon Route 53 Resources \(p. 655\)](#).

13. On the **Review and create** page, confirm that the settings that you specified on the previous pages are correct. If necessary, choose **Edit** for the applicable section, and update settings. When you're satisfied with the settings, choose **Create rule group**. The wizard takes you back to the **Rule groups** page where your new rule group is listed.

You now have a rule group that allows only specific domain queries through. To begin using it, you associate it with the VPCs where you want to use the filtering behavior. For more information, see [Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group \(p. 570\)](#).

Route 53 Resolver DNS Firewall block list example

In this tutorial, you'll create a rule group that blocks domains that you know to be malicious. The rule group allows all other outbound DNS requests over the Route 53 Resolver.

To configure a DNS Firewall block list by using the console wizard

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
- OR -
Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Rule groups**.
3. On the navigation bar, choose the Region for the rule group.
4. In the **Rule groups** page, choose **Add rule group**.
5. For the rule group name, enter **BlockListExample**. If you want an additional description, enter that as well.
6. Choose **Next**.
7. On the **Add rules** page, choose **Add rule**.
 - a. In the **Rule details** pane, enter the rule name **BlockList**.
 - b. In the **Domain list** pane, select **Add my own domain list**.
 - c. Under **Choose or create a new domain list**, select **Create new domain list**.
 - d. Enter a domain list name **MaliciousDomains**, then in the text box, enter the domains you want to block. For example, **example.org**. Enter one domain per line.

Note

If you want the rule to apply to subdomains as well, you must add those domains to the list also. For example, to add all of the example.org's subdomains, add ***.example.org** to the list.

- e. For the action, select **BLOCK** and then leave the response to send at the default setting of **NODATA**.
- f. Choose **Add rule**. The wizard displays the rule group's **Add rules** page with your **BlockList** rule listed.
8. Choose **Next**.
9. In the **Set rule priority** page, you can adjust the evaluation order of the rules in your rule group. DNS Firewall evaluates rules starting with the lowest priority setting, so the rule at the top of the list is the first one evaluated.

Select and adjust the rule ordering so that **BlockList** is evaluated either before or after any other rules you might have. Most of the time, known malicious domains should be blocked first. That is, the rules associated with them should have the lowest priority number.

10. In the **Add tags** page, you can optionally add a tag that you can use to search and filter your AWS resources.
11. Choose **Next** and then **Create rule group**.

You now have a rule group that blocks specific malicious domain queries. To begin using it, you associate it with the VPCs where you want to use the filtering behavior. For more information, see [Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group \(p. 570\)](#).

DNS Firewall rule groups and rules

This section describes the settings that you can configure for your DNS Firewall rule groups and rules, to define the DNS Firewall behavior for your VPCs. It also describes how to manage the settings for your rule groups and rules.

When you have your rule groups configured the way you want them, you use them directly and you can share and manage them between accounts and across your organization in AWS Organizations.

- You can associate a rule group with multiple VPCs, to provide consistent behavior across your organization. For information, see [Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group \(p. 570\)](#).
- You can share rule groups between accounts, for consistent DNS query management across your organization. For information, see [Sharing Route 53 Resolver DNS Firewall rule groups between AWS accounts \(p. 568\)](#).
- You can use rule groups across your organization in AWS Organizations by managing them in AWS Firewall Manager policies. For information about Firewall Manager, see [AWS Firewall Manager](#) in the [AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide](#).

Rule group settings in DNS Firewall

When you create or edit a DNS Firewall rule group, you specify the following values:

Name

A unique name that lets you easily find a rule group on the dashboard.

(Optional) Description

A short description that provides more context for the rule group.

Region

The AWS Region that you choose when you create the rule group. A rule group that you create in one Region is available only in that Region. To use the same rule group in more than one Region, you must create it in each Region.

Rules

The rule group filtering behavior is contained in its rules. For information, see the following section.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill. For more information about using tags for cost allocation, see [Using cost allocation tags](#) in the [AWS Billing and Cost Management User Guide](#).

Rule settings in DNS Firewall

When you create or edit a rule in a DNS Firewall rule group, you specify the following values:

Name

A unique identifier for the rule in the rule group.

(Optional) Description

A short description that provides more information about the rule.

Domain list

The list of domains that the rule inspects for. You can create and manage your own domain list or you can subscribe to a domain list that AWS manages for you. For more information, see [Route 53 Resolver DNS Firewall domain lists \(p. 563\)](#).

Action

How you want DNS Firewall to handle a DNS query whose domain name matches the specifications in the rule's domain list. For more information, see [Rule actions in DNS Firewall \(p. 561\)](#).

Priority

Unique positive integer setting for the rule within the rule group that determines processing order. DNS Firewall inspects DNS queries against the rules in a rule group starting with the lowest numeric priority setting and going up. You can change a rule's priority at any time, for example to change the order of processing or make space for other rules.

Rule actions in DNS Firewall

When DNS Firewall finds a match between a DNS query and a domain specification in a rule, it applies the action that's specified in the rule to the query.

You are required to specify one of the following options in each rule that you create:

- **Allow** – Stop inspecting the query and permit it to go through.
- **Alert** – Stop inspecting the query, permit it to go through, and log an alert for the query in the Route 53 Resolver logs.
- **Block** – Discontinue inspection of the query, block it from going to its intended destination, and log the block action for the query in the Route 53 Resolver logs.

Reply with the configured block response, from the following:

- **NODATA** – Respond indicating that the query was successful, but no response is available for it.
- **NXDOMAIN** – Respond indicating that the query's domain name doesn't exist.
- **OVERRIDE** – Provide a custom override in the response. This option requires the following additional settings:
 - **Record value** – The custom DNS record to send back in response to the query.
 - **Record type** – The DNS record's type. This determines the format of the record value. This must be CNAME.
 - **Time to live in seconds** – The recommended amount of time for the DNS resolver or web browser to cache the override record and use it in response to this query, if it is received again. By default, this is zero, and the record isn't cached.

For more information about the query logs configuration and the contents, see [Resolver query logging \(p. 619\)](#) and [Values that appear in Resolver query logs \(p. 622\)](#).

Use Alert to test blocking rules

When you first create a blocking rule, you can test it by configuring it with the action set to Alert. You can then look at the number of queries that the rule alerts on to see how many would be blocked if you set the action to Block.

Managing rule groups and rules in DNS Firewall

To manage rule groups and rules in the console, follow the guidance in this topic.

When you make changes to DNS Firewall entities, like rules and domain lists, DNS Firewall propagates the changes everywhere that the entities are stored and used. Your changes are applied within seconds, but there might be a brief period of inconsistency when the changes have arrived in some places and not in others. So, for example, if you add a domain to a domain list that's referenced by a blocking rule, the new domain might briefly be blocked in one area of your VPC while still allowed in another. This temporary inconsistency can occur when you first configure your rule group and VPC associations and when you change existing settings. Generally, any inconsistencies of this type last only a few seconds.

Creating a rule group and rules

To create a rule group and its rules

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

- OR -

Sign in to the AWS Management Console and open the

the Amazon VPC console under <https://console.aws.amazon.com/vpc/>.

2. In the navigation pane, choose **Rule groups**.
3. On the navigation bar, choose the Region for the rule group.
4. Choose **Add rule group**, then follow the wizard guidance to specify your rule group and rule settings.

For information about the values for rule groups, see [Rule group settings in DNS Firewall \(p. 560\)](#).

For information about the values for rules, see [Rule settings in DNS Firewall \(p. 561\)](#).

Viewing and updating a rule group and rules

To view and update a rule group

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

- OR -

Sign in to the AWS Management Console and open the

the Amazon VPC console under <https://console.aws.amazon.com/vpc/>.

2. In the navigation pane, choose **Rule groups**.
3. On the navigation bar, choose the Region for the rule group.
4. Select the rule group that you want to view or edit, then choose **View details**.

5. In the rule group's page, you can view and edit settings.

For information about the values for rule groups, see [Rule group settings in DNS Firewall \(p. 560\)](#).

For information about the values for rules, see [Rule settings in DNS Firewall \(p. 561\)](#).

Deleting a rule group

To delete a rule group, perform the following procedure.

Important

If you delete a rule group that's associated with a VPC, DNS Firewall removes the association and stops the protections that the rule group was providing to the VPC.

Deleting DNS Firewall entities

When you delete an entity that you can use in DNS Firewall, like a domain list that might be in use in a rule group, or a rule group that might be associated with a VPC, DNS Firewall checks to see if the entity is currently being used. If it finds that it is in use, DNS Firewall warns you. DNS Firewall is almost always able to determine if an entity is in use. However, in rare cases it might not be able to do so. If you need to be sure that nothing is currently using the entity, check for it in your DNS Firewall configurations before deleting it. If the entity is a referenced domain list, check that no rule groups are using it. If the entity is a rule group, check that it is not associated with any VPCs.

To delete a rule group

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
- OR -
Sign in to the AWS Management Console and open the
the Amazon VPC console under <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Rule groups**.
3. On the navigation bar, choose the Region for the rule group.
4. Select the rule group that you want to delete, then choose **Delete**, and confirm the deletion.

Route 53 Resolver DNS Firewall domain lists

A *domain list* is a reusable set of domain specifications that you use in a DNS Firewall rule, inside a rule group. When you associate a rule group with a VPC, DNS Firewall compares your DNS queries against the domain lists that are used in the rules. If it finds a match, it handles the DNS query according to the matching rule's action. For more information about rule groups and rules, see [DNS Firewall rule groups and rules \(p. 560\)](#).

Domain lists allow you to separate your explicit domain specifications from the actions that you want to take on them. You can use a single domain list in multiple rules and any updates that you do to the domain list automatically affects all rules that use it.

Domain lists fall into two main categories:

- Managed domain lists, which AWS creates and maintains for you.
- Your own domain lists, which you create and maintain.

This section describes the types of managed domain lists that are available to you and provides guidance for creating and managing your own domain lists, if you choose to do so.

Managed domain lists

Managed domain lists contain domain names that are associated with malicious activity or other potential threats. AWS maintains these lists to enable Route 53 Resolver customers to check outbound DNS queries against them for free when using DNS Firewall.

Keeping up to date on the constantly changing threat landscape can be time consuming and expensive. Managed domain lists can save you time when you implement and use DNS Firewall. AWS automatically updates managed domain lists when new vulnerabilities and threats emerge. AWS is often notified of new vulnerabilities before public disclosure, so DNS Firewall can deploy mitigations for you even, often before a new threat becomes widely known.

AWS Managed Domain Lists are designed to help protect you from common web threats and they add another layer of security for your applications. However, AWS Managed Domain Lists aren't intended as a replacement for other security controls, such as Amazon GuardDuty, which are determined by the AWS resources that you select.

AWS Managed Domain Lists are not currently available in all Regions. The following table lists the Region availability.

Managed domain list Region availability

Region	Managed domain lists available?
Asia Pacific (Mumbai)	Yes
Asia Pacific (Seoul)	Yes
Asia Pacific (Singapore)	Yes
Asia Pacific (Sydney)	Yes
Asia Pacific (Tokyo)	Yes
Asia Pacific (Osaka) Region	Yes
Canada (Central) Region	Yes
Europe (Frankfurt) Region	Yes
Europe (Ireland) Region	Yes
Europe (London) Region	Yes
Europe (Paris) Region	Yes
Europe (Stockholm)	Yes
South America (São Paulo)	Yes
US East (N. Virginia)	Yes
US East (Ohio)	Yes
US West (N. California)	Yes
US West (Oregon)	Yes

Region	Managed domain lists available?
AWS GovCloud (US)	No
Asia Pacific (Hong Kong)	No
Middle East (Bahrain)	No
Africa (Cape Town)	No
Europe (Milan)	No

Available AWS Managed Domain Lists

This section describes the AWS Managed Domain Lists that are currently available. When you're in a Region where these domain lists are supported, you see them on the console when you manage domain lists and when you specify the domain list for a rule. In the logs, the domain list is logged within the `firewall_domain_list_id` field.

AWS provides the following managed domain lists, in the Regions they are available, for all users of Route 53 Resolver DNS Firewall.

- `AWSManagedDomainsMalwareDomainList` -- Domains associated with sending malware, hosting malware, or distributing malware.
- `AWSManagedDomainsBotnetCommandandControl` – Domains associated with controlling networks of computers that are infected with spamming malware.

Managed domain lists cannot be downloaded or browsed. To protect intellectual property, you can't view or edit the individual domain specifications within a domain list. This restriction also helps to prevent malicious users from designing threats that specifically to circumvent published lists.

For more information about managed domain lists, contact the [AWS Support Center](#).

As a best practice, before using a managed domain list in production, test it in a non-production environment, with the rule action set to `Alert`. Evaluate the rule using Amazon CloudWatch metrics combined with Route 53 Resolver DNS Firewall sampled requests or DNS Firewall logs. When you're satisfied that the rule does what you want, change the action setting as needed.

Additional security considerations

AWS Managed Domain Lists are designed to help protect you from common web threats. When used in accordance with the documentation, AWS Managed Domain Lists add another layer of security for your applications. However, AWS Managed Domain Lists aren't intended as a replacement for other security controls, which are determined by the AWS resources that you select. To ensure that your resources in AWS are properly protected, see the guidance at [Shared Responsibility Model](#).

Mitigating false positive scenarios

If you are encountering false-positive scenarios in rules that use AWS Managed Domain Lists to block queries, perform the following steps:

1. In the Resolver logs, identify the rule group and managed domain list that are causing the false positive. You do this by finding the log for the query that DNS Firewall is blocking, but that you want to allow through. The log record lists the rule group, rule action, and the managed domain list. For information about the logs, see [Values that appear in Resolver query logs \(p. 622\)](#).
2. Create a new rule in the rule group that explicitly allows the blocked query through. When you create the rule, you can define your own domain list with just the domain specification that you

want to allow. Follow the guidance for rule group and rule management at [Creating a rule group and rules \(p. 562\)](#).

3. Prioritize the new rule inside the rule group so that it runs before the rule that's using the managed domain list. To do this, give the new rule a lower numeric priority setting.

When you have updated your rule group, the new rule will explicitly allow the domain name that you want to allow before the blocking rule runs.

Managing your own domain lists

You can create your own domain lists to specify domain categories that you either don't find in the managed domain list offerings or that you prefer to handle on your own.

In addition to the procedures described in this section, in the console, you can create a domain list in the context of Route 53 Resolver DNS Firewall rule management, when you create or update a rule.

Each domain specification in your domain list must satisfy the following requirements:

- It can optionally start with * (asterisk).
- With the exception of the optional starting asterisk, it must only contain the following characters: A–Z, a–z, 0–9, – (hyphen).
- It must be from 1–255 characters in length.

When you make changes to DNS Firewall entities, like rules and domain lists, DNS Firewall propagates the changes everywhere that the entities are stored and used. Your changes are applied within seconds, but there might be a brief period of inconsistency when the changes have arrived in some places and not in others. So, for example, if you add a domain to a domain list that's referenced by a blocking rule, the new domain might briefly be blocked in one area of your VPC while still allowed in another. This temporary inconsistency can occur when you first configure your rule group and VPC associations and when you change existing settings. Generally, any inconsistencies of this type last only a few seconds.

Test your domain list before using it in production

As a best practice, before using a domain list in production, test it in a non-production environment, with the rule action set to Alert. Evaluate the rule using Amazon CloudWatch metrics and the Resolver logs. The logs provide the domain list name for all alerts and blocking actions. When you're satisfied that the domain list is matching your DNS queries the way you want it to, change the rule action setting as needed. For information about CloudWatch metrics and the query logs, see [Monitoring Route 53 Resolver DNS Firewall rule groups with Amazon CloudWatch \(p. 633\)](#), [Values that appear in Resolver query logs \(p. 622\)](#), and [Managing Resolver query logging configurations \(p. 621\)](#).

To add a domain list

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
- OR -
Sign in to the AWS Management Console and open the
the Amazon VPC console under <https://console.aws.amazon.com/vpc/>.
2. Choose **Domain lists**. In the **Domain lists** page, you can select and edit existing domain lists and you can add your own.
3. To add a domain list, choose **Add domain list**.
4. Provide a name for your domain list, and then enter your domain specifications in the text box, one per line.

If you slide **Switch to bulk upload** to **on**, enter the URI of the Amazon S3 bucket where you created a domain list. This domain list should have one domain name per line.

5. Choose **Add domain list**. The **Domain lists** page lists your new domain list.

After you create the domain list, you can reference it by name from your DNS Firewall rules.

Deleting DNS Firewall entities

When you delete an entity that you can use in DNS Firewall, like a domain list that might be in use in a rule group, or a rule group that might be associated with a VPC, DNS Firewall checks to see if the entity is currently being used. If it finds that it is in use, DNS Firewall warns you. DNS Firewall is almost always able to determine if an entity is in use. However, in rare cases it might not be able to do so. If you need to be sure that nothing is currently using the entity, check for it in your DNS Firewall configurations before deleting it. If the entity is a referenced domain list, check that no rule groups are using it. If the entity is a rule group, check that it is not associated with any VPCs.

To delete a domain list

1. In the navigation pane, choose **Domain lists**.
2. On the navigation bar, choose the Region for the domain list.
3. Select the domain list that you want to delete, then choose **Delete**, and confirm the deletion.

Configuring logging for DNS Firewall

You can evaluate your DNS Firewall rules by using Amazon CloudWatch metrics and the Resolver query logs. The logs provide the domain list name for all alerts and blocking actions. For more information about Amazon CloudWatch, see [Monitoring Route 53 Resolver DNS Firewall rule groups with Amazon CloudWatch \(p. 633\)](#).

When you enable DNS Firewall, associate it to a VPC, and you have logging enabled, `firewall_rule_group_id`, `firewall_rule_action`, and `firewall_domain_list_id` are the DNS Firewall specific fields provided within your logs.

To start logging the DNS queries that are filtered by DNS Firewall rules that originate in your VPCs, you perform the following tasks in the Amazon Route 53 console:

To configure Resolver query logging for DNS Firewall

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Expand the Route 53 console menu. In the upper left corner of the console, choose the three horizontal bars (≡) icon.
3. Within the Resolver menu, choose **Query logging**.
4. In the Region selector, choose the AWS Region where you want to create the query logging configuration.

This must be the same Region where you created the VPCs that are associated with DNS Firewall that you want to log queries for. If you have VPCs in multiple Regions, you must create at least one query logging configuration for each Region.

5. Choose **Configure query logging**.
6. Specify the following values:

Query logging configuration name

Enter a name for your query logging configuration. The name appears in the console in the list of query logging configurations. Enter a name that will help you find this configuration later.

Query logs destination

Choose the type of AWS resource that you want Resolver to send query logs to. For information about how to choose among the options (CloudWatch Logs log group, S3 bucket, and Kinesis Data Firehose delivery stream), see [AWS resources that you can send Resolver query logs to \(p. 620\)](#).

After you choose the type of resource, you can either create another resource of that type or choose an existing resource that was created by the current AWS account.

Note

You can choose only resources that were created in the AWS Region that you chose in step 4, the Region where you're creating the query logging configuration. If you choose to create a new resource, that resource will be created in the same Region.

VPCs to log queries for

This query logging configuration will log DNS queries that originate in the VPCs that you choose. Check the check box for each VPC in the current Region that you want Resolver to log queries for, then choose **Choose**.

Note

VPC log delivery can be enabled only once for a specific destination type. The logs can't be delivered to multiple destinations of the same type. For example, VPC logs can't be delivered to two Amazon S3 destinations.

7. Choose **Configure query logging**.

Note

You should start to see DNS queries made by resources in your VPC in the logs within a few minutes of successfully creating the query logging configuration.

Sharing Route 53 Resolver DNS Firewall rule groups between AWS accounts

You can share DNS Firewall rule groups between AWS accounts. To share rule groups, you use AWS Resource Access Manager (AWS RAM). The DNS Firewall console integrates with the AWS RAM console. For more information about AWS RAM, see the [Resource Access Manager User Guide](#).

Note the following:

Associating shared rule groups with VPCs

If another AWS account has shared a rule group with your account, you can associate it with your VPCs the same way that you associate rule groups that you've created. For more information, see [Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group \(p. 570\)](#).

Deleting or unsharing a shared rule group

If you share a rule group with other accounts and then either delete the rule group or stop sharing it, DNS Firewall removes all associations that the other accounts created between the rule group and their VPCs.

Maximum settings for rule groups and associations

Shared rule groups and their associations with VPCs are included in the counts for the accounts with which the rule groups are shared.

For current DNS Firewall quotas, see [Quotas on Route 53 Resolver DNS Firewall \(p. 674\)](#).

Permissions

To share a rule group with another AWS account, you must have permission to use the [PutFirewallRuleGroupPolicy](#) action.

Restrictions on the AWS account that a rule group is shared with

The account that a rule group is shared with can't change or delete the rule group.

Tagging

Only the account that created a rule group can add, delete, or see tags on the rule group.

To view the current sharing status of a rule group (including the account that shared the rule group or the account that a rule group is shared with), and to share rule groups with another account, perform the following procedure.

To view sharing status and share rule groups with another AWS account

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Rule groups**.
3. On the navigation bar, choose the Region where you created the rule group.

The **Sharing status** column shows the current sharing status of rule groups that were created by the current account or that are shared with the current account:

- **Not shared:** The current AWS account created the rule group, and the rule group is not shared with any other accounts.
 - **Shared by me:** The current account created the rule group and shared it with one or more accounts.
 - **Shared with me:** Another account created the rule group and shared it with the current account.
4. Choose the name of the rule group that you want to display sharing information for or that you want to share with another account.

On the **Rule group: rule group name** page, the value under **Owner** displays the ID of the account that created the rule group. That's the current account unless the value of **Sharing status** is **Shared with me**. In that case, **Owner** is the account that created the rule group and shared it with the current account.

5. Choose **Share** to view additional information or to share the rule group with another account. A page in the AWS RAM console appears, depending on the value of **Sharing status**:
 - **Not shared:** The **Create resource share** page appears. For information about how to share the rule group with another account, organizational unit (OU), or organization, go to the step that follows this one.
 - **Shared by me:** The **Shared resources** page shows the rule groups and other resources that are owned by the current account and shared with other accounts.
 - **Shared with me:** The **Shared resources** page shows the rule groups and other resources that are owned by other accounts and shared with the current account.
6. To share a rule group with another AWS account, OU, or organization, specify the following values.

Note

You can't update sharing settings. To change any of the following settings, you must reshare a rule group with the new settings and then remove the old sharing settings.

Description

Enter a short description that helps you remember why you shared the rule group.

Resources

Choose the check box for the rule group that you want to share.

Principals

Enter the AWS account number, OU name, or organization name.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill; you can use also tags for other purposes. For more information about using tags for cost allocation, see [Using cost allocation tags](#) in the *AWS Billing and Cost Management User Guide*.

Enabling Route 53 Resolver DNS Firewall protections for your VPC

You enable DNS Firewall protections for your VPC by associating one or more rule groups with the VPC. Whenever a VPC is associated with a DNS Firewall rule group, Route 53 Resolver provides the following DNS Firewall protections:

- Resolver routes the VPC's outbound DNS queries through DNS Firewall, and DNS Firewall filters the queries using the associated rule groups.
- Resolver enforces the settings in the VPC's DNS Firewall configuration.

To provide DNS Firewall protections to your VPC, you do the following:

- Create and manage associations between your DNS Firewall rule groups and your VPC. For information about rule groups, see [DNS Firewall rule groups and rules \(p. 560\)](#).
- Configure how you want Resolver to handle DNS queries for the VPC during a failure, for example if DNS Firewall doesn't provide a response for a DNS query.

Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group

To view a rule group's VPC associations

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

- OR -

Sign in to the AWS Management Console and open the

- the Amazon VPC console under <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Rule groups**.
 3. On the navigation bar, choose the Region for the rule group.
 4. Select the rule group that you want to associate.
 5. Choose **View details**. The rule group page displays.
 6. Toward the bottom, you can see a tabbed details area that includes rules and associated VPCs. Choose the tab **Associated VPCs**.

To associate a rule group with a VPC

1. Locate the rule group's VPC associations by following the instructions in [the preceding procedure \(p. 568\) To view a rule group's VPC associations](#).
2. In the **Associated VPCs** tab, choose **Associate VPC**.
3. Locate the VPC that you want to associate with the rule group in the dropdown. Select it, then choose **Associate**.

In the rule group page, your VPC is listed in the **Associated VPCs** tab. At first, the association's **Status** reports **Updating**. When the association is complete, the status changes to **Complete**.

To remove an association between a rule group and a VPC

1. Locate the rule group's VPC associations by following the instructions in [the preceding procedure \(p. 568\) To view a rule group's VPC associations](#).
2. Select the VPC that you want to remove from the list, then choose **Disassociate**. Verify, and then confirm the action.

On the rule group page, your VPC is listed in the **Associated VPCs** tab with the status of **Disassociating**. When the operation completes, DNS Firewall updates the list to remove the VPC.

DNS Firewall VPC configuration

The DNS Firewall configuration for your VPC determines whether Route 53 Resolver allows queries through or blocks them during failures, for example when DNS Firewall is impaired, unresponsive, or not available in the zone. Resolver enforces a VPC's firewall configuration whenever you have one or more DNS Firewall rule groups associated with the VPC.

You can configure a VPC to fail open or fail closed.

- By default, the failure mode is closed, which means that Resolver blocks any queries for which it doesn't receive a reply from DNS Firewall and sends a `SERVFAIL` DNS response. This approach favors security over availability.
- If you enable fail open, Resolver allows queries through if it doesn't receive a reply from DNS Firewall. This approach favors availability over security.

To change the DNS Firewall configuration for a VPC (console)

1. Sign in to the AWS Management Console and open the Resolver console at <https://console.aws.amazon.com/route53resolver/>.
2. In the navigation pane under **Resolvers**, choose **VPCs**.
3. In the **VPCs** page, locate and edit the VPC. Change the DNS Firewall configuration to fail open or fail closed as needed.

To change the DNS Firewall behavior for a VPC (API)

- Update your VPC firewall configuration by calling [UpdateFirewallConfig](#) and enabling or disabling `FirewallFailOpen`.

You can retrieve a list of your VPC firewall configurations through the API by calling [ListFirewallConfigs](#).

Security in Amazon Route 53

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security of the cloud and security *in the cloud*:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS compliance programs](#). To learn about the compliance programs that apply to Amazon Route 53, see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Route 53. The following topics show you how to configure Route 53 to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Route 53 resources.

Topics

- [Data protection in Route 53 \(p. 573\)](#)
- [Identity and access management in Amazon Route 53 \(p. 574\)](#)
- [Logging and monitoring in Amazon Route 53 \(p. 612\)](#)
- [Compliance validation for Amazon Route 53 \(p. 613\)](#)
- [Resilience in Amazon Route 53 \(p. 613\)](#)
- [Infrastructure security in Amazon Route 53 \(p. 614\)](#)

Data protection in Route 53

The AWS [shared responsibility model](#) applies to data protection in Amazon Route 53. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the [AWS Security Blog](#).

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.

- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with Route 53 or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Protection from dangling delegation records in Route 53

In Route 53, when you use nameserver (NS) records to delegate the management of a subdomain to another public hosted zone, a problem could arise if the subdomain hosted zone is deleted without also deleting the delegation. Another user could potentially re-create the subdomain hosted zone and gain control via the still-active delegation belonging to the first customer. However, Route 53 protects against such "dangling" delegations by not allowing any new hosted zones with overlapping domain names to be created by using those nameservers before verifying that the delegation has first been removed.

Identity and access management in Amazon Route 53

To perform any operation on Amazon Route 53 resources, such as registering a domain or updating a record, AWS Identity and Access Management (IAM) requires you to authenticate that you're an approved AWS user. If you're using the Route 53 console, you authenticate your identity by providing your AWS user name and a password. If you're accessing Route 53 programmatically, your application authenticates your identity for you by using access keys or by signing requests.

After you authenticate your identity, IAM controls your access to AWS by verifying that you have permissions to perform operations and to access resources. If you are an account administrator, you can use IAM to control the access of other users to the resources that are associated with your account.

This chapter explains how to use [IAM](#) and Route 53 to help secure your resources.

Topics

- [Authentication \(p. 574\)](#)
- [Access control \(p. 575\)](#)

Authentication

You can access AWS as any of the following types of identities:

- **AWS account root user** – When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the [best practice of using the root user only to create your first IAM user](#). Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.
- **IAM user** – An [IAM user](#) is an identity within your AWS account that has specific custom permissions (for example, permissions to create a hosted zone in Route 53). You can use an IAM user name and password to sign in to secure AWS webpages like the [AWS Management Console](#), [AWS Discussion Forums](#), or the [AWS Support Center](#).

In addition to a user name and password, you can also generate [access keys](#) for each user. You can use these keys when you access AWS services programmatically, either through [one of the several SDKs](#) or by using the [AWS Command Line Interface \(CLI\)](#). The SDK and CLI tools use the access keys to cryptographically sign your request. If you don't use AWS tools, you must sign the request yourself. Route 53 supports *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see [Signature Version 4 signing process](#) in the [AWS General Reference](#).

- **IAM role** – An [IAM role](#) is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session. IAM roles with temporary credentials are useful in the following situations:
 - **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an [identity provider](#). For more information about federated users, see [Federated users and roles](#) in the [IAM User Guide](#).
 - **AWS service access** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the [IAM User Guide](#).
 - **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the [IAM User Guide](#).

Access control

To create, update, delete, or list Amazon Route 53 resources, you need permissions to perform the operation, and you need permission to access the corresponding resources. In addition, to perform the operation programmatically, you need valid access keys.

The following sections describe how to manage permissions for Route 53. We recommend that you read the overview first.

- [Overview of managing access permissions to your Amazon Route 53 resources \(p. 576\)](#)
- [Using identity-based policies \(IAM policies\) for Amazon Route 53 \(p. 579\)](#)
- [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#)

Overview of managing access permissions to your Amazon Route 53 resources

Every AWS resource is owned by an AWS account, and permissions to create or access a resource are governed by permissions policies.

Note

An *account administrator* (or administrator user) is a user that has administrator privileges. For more information about administrators, see [IAM best practices](#) in the *IAM User Guide*.

When you grant permissions, you decide who gets the permissions, the resources they get permissions for, and the actions that they get permissions to perform.

Topics

- [ARNs for Amazon Route 53 resources \(p. 576\)](#)
- [Understanding resource ownership \(p. 576\)](#)
- [Managing access to resources \(p. 577\)](#)
- [Specifying policy elements: Resources, actions, effects, and principals \(p. 578\)](#)
- [Specifying conditions in a policy \(p. 579\)](#)

ARNs for Amazon Route 53 resources

Amazon Route 53 supports a variety of resource types for DNS, health checking, and domain registration. In a policy, you can grant or deny access to the following resources by using * for the ARN:

- Health checks
- Hosted zones
- Reusable delegation sets
- Status of a resource record set change batch (API only)
- Traffic policies (traffic flow)
- Traffic policy instances (traffic flow)

Not all Route 53 resources support permissions. You can't grant or deny access to the following resources:

- Domains
- Individual records
- Tags for domains
- Tags for health checks
- Tags for hosted zones

Route 53 provides API actions to work with each of these types of resources. For more information, see the [Amazon Route 53 API Reference](#). For a list of actions and the ARN that you specify to grant or deny permission to use each action, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#).

Understanding resource ownership

An AWS account owns the resources that are created in the account, regardless of who created the resources. Specifically, the resource owner is the AWS account of the principal entity (that is, the root account, an IAM user, or an IAM role) that authenticates the resource creation request.

The following examples illustrate how this works:

- If you use the root account credentials of your AWS account to create a hosted zone, your AWS account is the owner of the resource.
- If you create an IAM user in your AWS account and grant permissions to create a hosted zone to that user, the user can create a hosted zone. However, your AWS account, to which the user belongs, owns the hosted zone resource.
- If you create an IAM role in your AWS account with permissions to create a hosted zone, anyone who can assume the role can create a hosted zone. Your AWS account, to which the role belongs, owns the hosted zone resource.

Managing access to resources

A *permissions policy* specifies who has access to what. This section explains the options for creating permissions policies for Amazon Route 53. For general information about IAM policy syntax and descriptions, see the [AWS IAM Policy Reference](#) in the *IAM User Guide*.

Policies attached to an IAM identity are referred to as *identity-based* policies (IAM policies), and policies attached to a resource are referred to as *resource-based* policies. Route 53 supports only identity-based policies (IAM policies).

Topics

- [Identity-based policies \(IAM policies\) \(p. 577\)](#)
- [Resource-based policies \(p. 578\)](#)

Identity-based policies (IAM policies)

You can attach policies to IAM identities. For example, you can do the following:

- **Attach a permissions policy to a user or a group in your account** – An account administrator can use a permissions policy that is associated with a particular user to grant permissions for that user to create Amazon Route 53 resources.
- **Attach a permissions policy to a role (grant cross-account permissions)** – You can grant permission to perform Route 53 actions to a user that was created by another AWS account. To do so, you attach a permissions policy to an IAM role, and then you allow the user in the other account to assume the role. The following example explains how this works for two AWS accounts, account A and account B:
 1. Account A administrator creates an IAM role and attaches to the role a permissions policy that grants permissions to create or access resources that are owned by account A.
 2. Account A administrator attaches a trust policy to the role. The trust policy identifies account B as the principal that can assume the role.
 3. Account B administrator can then delegate permissions to assume the role to users or groups in Account B. This allows users in account B to create or access resources in account A.

For more information about how to delegate permissions to users in another AWS account, see [Access management](#) in the *IAM User Guide*.

The following example policy allows a user to perform the `CreateHostedZone` action to create a public hosted zone for any AWS account:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "route53:CreateHostedZone",  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "Action": [
            "route53:CreateHostedZone"
        ],
        "Resource": "*"
    },
]
}
```

If you want the policy to also apply to private hosted zones, you need to grant permissions to use the `Route 53 AssociateVPCWithHostedZone` action and two Amazon EC2 actions, `DescribeVpcs` and `DescribeRegion`, as shown in the following example:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information about attaching policies to identities for Route 53, see [Using identity-based policies \(IAM policies\) for Amazon Route 53 \(p. 579\)](#). For more information about users, groups, roles, and permissions, see [Identities \(users, groups, and roles\)](#) in the *IAM User Guide*.

Resource-based policies

Other services, such as Amazon S3, also support attaching permissions policies to resources. For example, you can attach a policy to an S3 bucket to manage access permissions to that bucket. Amazon Route 53 doesn't support attaching policies to resources.

Specifying policy elements: Resources, actions, effects, and principals

Amazon Route 53 includes API actions (see the [Amazon Route 53 API Reference](#)) that you can use on each Route 53 resource (see [ARNs for Amazon Route 53 resources \(p. 576\)](#)). You can grant a user or a federated user permissions to perform any or all of these actions. Note that some API actions, such as registering a domain, require permissions to perform more than one action.

The following are the basic policy elements:

- **Resource** – You use an Amazon Resource Name (ARN) to identify the resource that the policy applies to. For more information, see [ARNs for Amazon Route 53 resources \(p. 576\)](#).
- **Action** – You use action keywords to identify resource operations that you want to allow or deny. For example, depending on the specified `Effect`, the `route53:CreateHostedZone` permission allows or denies a user the ability to perform the Route 53 `CreateHostedZone` action.

- **Effect** – You specify the effect, either allow or deny, when a user tries to perform the action on the specified resource. If you don't explicitly grant access to an action, access is implicitly denied. You can also explicitly deny access to a resource, which you might do to make sure that a user cannot access it, even if a different policy grants access.
- **Principal** – In identity-based policies (IAM policies), the user that the policy is attached to is the implicit principal. For resource-based policies, you specify the user, account, service, or other entity that you want to receive permissions (applies to resource-based policies only). Route 53 doesn't support resource-based policies.

For more information about IAM policy syntax and descriptions, see the [AWS IAM Policy Reference](#) in the *IAM User Guide*.

For a list showing all of the Route 53 API operations and the resources that they apply to, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#).

Specifying conditions in a policy

When you grant permissions, you can use the IAM policy language to specify when a policy should take effect. For example, you might want a policy to be applied only after a specific date. For more information about specifying conditions in a policy language, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.

To express conditions, you use predefined condition keys. There are no condition keys specific to Route 53. However, there are AWS wide condition keys that you can use as needed. For a complete list of AWS wide keys, see [Available keys for conditions](#) in the *IAM User Guide*.

Using identity-based policies (IAM policies) for Amazon Route 53

This topic provides examples of identity-based policies that demonstrate how an account administrator can attach permissions policies to IAM identities (users, groups, and roles) and thereby grant permissions to perform operations on Amazon Route 53 resources.

Important

We recommend that you first review the introductory topics that explain the basic concepts and options to manage access to your Route 53 resources. For more information, see [Overview of managing access permissions to your Amazon Route 53 resources \(p. 576\)](#).

Note

When granting access, the hosted zone and the Amazon VPC must belong to the same partition. A partition is a group of AWS Regions. Each AWS account is scoped to one partition.

The following are the supported partitions:

- aws - AWS Regions
- aws-cn - China Regions
- aws-us-gov - AWS GovCloud (US) Region

For more information, see [Access Management](#) in the *AWS General Reference*.

Topics

- [Permissions required to use the Amazon Route 53 console \(p. 580\)](#)
- [Example permissions for a domain record owner \(p. 583\)](#)
- [Route 53 customer managed key permissions required for DNSSEC signing \(p. 583\)](#)
- [Customer managed policy examples \(p. 585\)](#)

The following example shows a permissions policy. The `Sid`, or statement ID, is optional:

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

The policy includes two statements:

- The first statement grants permissions to the actions that are required to create and manage public hosted zones and their records. The wildcard character (*) in the Amazon Resource Name (ARN) grants access to all the hosted zones that are owned by the current AWS account.
- The second statement grants permissions to all the actions that are required to create and manage health checks.

For a list of actions and the ARN that you specify to grant or deny permission to use each action, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#).

Permissions required to use the Amazon Route 53 console

To grant full access to the Amazon Route 53 console, you grant the permissions in the following permissions policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "
```

```

    "Action": [
        "route53:*",
        "route53domains:*",
        "cloudfront>ListDistributions",
        "elasticloadbalancingDescribeLoadBalancers",
        "elasticbeanstalkDescribeEnvironments",
        "s3>ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "ec2DescribeRegions",
        "ec2DescribeVpcs",
        "ec2>CreateNetworkInterface",
        "ec2>CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2DescribeAvailabilityZones",
        "ec2DescribeNetworkInterfaces",
        "ec2DescribeSecurityGroups",
        "ec2DescribeSubnets",
        "ec2ModifyNetworkInterfaceAttribute",
        "sns>ListTopics",
        "sns>ListSubscriptionsByTopic",
        "sns>CreateTopic",
        "kms>ListAliases",
        "kmsDescribeKey",
        "kmsCreateKey",
        "kmsCreateAlias",
        "kmsSign",
        "cloudwatchDescribeAlarms",
        "cloudwatchPutMetricAlarm",
        "cloudwatchDeleteAlarms",
        "cloudwatchGetMetricStatistics"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": "arn:aws:apigateway:*/::/domainnames"
}
]
}

```

Here's why the permissions are required:

route53:*

Lets you perform all Route 53 actions *except* the following:

- Create and update alias records for which the value of **Alias Target** is a CloudFront distribution, an Elastic Load Balancing load balancer, an Elastic Beanstalk environment, or an Amazon S3 bucket. (With these permissions, you can create alias records for which the value of **Alias Target** is another record in the same hosted zone.)
- Work with private hosted zones.
- Work with domains.
- Create, delete, and view CloudWatch alarms.
- Render CloudWatch metrics in the Route 53 console.

route53domains:*

Lets you work with domains.

Important

If you list route53 actions individually, you must include `route53:CreateHostedZone` to work with domains. When you register a domain, a hosted zone is created at the same time,

so a policy that includes permissions to register domains also requires permission to create hosted zones.

For domain registration, Route 53 doesn't support granting or denying permissions to individual resources.

route53resolver:*

Lets you work with Route 53 Resolver.

cloudfront>ListDistributions

Lets you create and update alias records for which the value of **Alias Target** is a CloudFront distribution.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of distributions to display in the console.

elasticloadbalancing:DescribeLoadBalancers

Lets you create and update alias records for which the value of **Alias Target** is an ELB load balancer.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of load balancers to display in the console.

elasticbeanstalk:DescribeEnvironments

Lets you create and update alias records for which the value of **Alias Target** is an Elastic Beanstalk environment.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of environments to display in the console.

s3>ListAllMyBuckets, s3:GetBucketLocation, and s3:GetBucketWebsite

Let you create and update alias records for which the value of **Alias Target** is an Amazon S3 bucket. (You can create an alias to an Amazon S3 bucket only if the bucket is configured as a website endpoint; `s3:GetBucketWebsite` gets the required configuration information.)

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of buckets to display in the console.

ec2:DescribeVpcs and ec2:DescribeRegions

Lets you work with private hosted zones.

All listed ec2 permissions

Lets you work with Route 53 Resolver.

**sns>ListTopics, sns>ListSubscriptionsByTopic, sns>CreateTopic,
cloudwatch:DescribeAlarms, cloudwatch:PutMetricAlarm, cloudwatch>DeleteAlarms**

Lets you create, delete, and view CloudWatch alarms.

cloudwatch:GetMetricStatistics

Lets you create CloudWatch metric health checks.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get statistics to display in the console.

apigateway:GET

Lets you create and update alias records for which the value of **Alias Target** is an Amazon API Gateway API.

This permission isn't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of APIs to display in the console.

kms : *

Lets you work with AWS KMS to enable DNSSEC signing.

Example permissions for a domain record owner

In some scenarios, a hosted zone owner might be responsible for the overall management of the hosted zone, while another person in the organization is responsible for a subset of those tasks. A hosted zone owner who has enabled DNSSEC signing, for example, might want to create an IAM policy that includes the permission for someone else to add and delete Resource Set Records (RRs) in the hosted zone, among other tasks. The specific permissions that a hosted zone owner chooses to enable for a record owner or other people will depend on their organization's policy.

The following is an example IAM policy that allows a record owner to make modifications to RRs, traffic policies, and health checks. A record owner with this policy is not allowed to do zone-level operations, such as creating or deleting a zone, enabling or disabling query logging, creating or deleting a reusable delegation set, or changing DNSSEC settings.

```
{  
    "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 customer managed key permissions required for DNSSEC signing

When you enable DNSSEC signing for Route 53, Route 53 creates a key-signing key (KSK) based on a customer managed key in AWS Key Management Service (AWS KMS). You can use an existing customer managed key that supports DNSSEC signing or create a new one. Route 53 must have permission to access your customer managed key so that it can create the KSK for you.

To enable Route 53 to access your customer managed key, make sure that your customer managed key policy contains the following statements:

```
{  
    "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
        }
    }
}

```

The confused deputy problem is a security issue where an entity without a permission for an action can coerce a more-privileged entity to perform it. To protect your AWS KMS from it, you can optionally limit the permissions that a service has to a resource in a resource-based policy by supplying a combination of `aws:SourceAccount` and `aws:SourceArn` conditions (both or one). `aws:SourceAccount` is an AWS account ID of an owner of a hosted zone. `aws:SourceArn` is an ARN of a hosted zone.

The following are two examples of permissions you can add:

```

{
    "Sid": "Allow Route 53 DNSSEC Service",
    ...
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53::::hostedzone/HOSTED_ZONE_ID"
        }
    }
},

```

- Or -

```

{
    "Sid": "Allow Route 53 DNSSEC Service",
    ...
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": [ "1111-2222-3333", "4444-5555-6666" ]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53::::hostedzone/*"
        }
    }
},

```

For more information, see [The confused deputy problem](#) in the *IAM User Guide*.

Customer managed policy examples

You can create your own custom IAM policies to allow permissions for Route 53 actions. You can attach these custom policies to the IAM users or groups that require the specified permissions. These policies work when you are using the Route 53 API, the AWS SDKs, or the AWS CLI. The following examples show permissions for several common use cases. For the policy that grants a user full access to Route 53, see [Permissions required to use the Amazon Route 53 console \(p. 580\)](#).

Examples

- Example 1: Allow read access to all hosted zones (p. 585)
 - Example 2: Allow creation and deletion of hosted zones (p. 585)
 - Example 3: Allow full access to all domains (public hosted zones only) (p. 586)
 - Example 4: Allow creation of inbound and outbound Route 53 Resolver endpoints (p. 586)

Example 1: Allow read access to all hosted zones

The following permissions policy grants the user permissions to list all hosted zones and view all the records in a hosted zone.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "route53:GetHostedZone",  
                "route53>ListResourceRecordSets"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": ["route53>ListHostedZones"],  
            "Resource": "*"  
        }  
    ]  
}
```

Example 2: Allow creation and deletion of hosted zones

The following permissions policy allows users to create and delete hosted zones, and to track the progress of the change.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["route53:CreateHostedZone"],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": ["route53:DeleteHostedZone"],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": ["route53:ListHostedZones"],  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "Action": ["route53:GetChange"],
        "Resource": "*"
    }
}
```

Example 3: Allow full access to all domains (public hosted zones only)

The following permissions policy allows users to perform all actions on domain registrations, including permissions to register domains and create hosted zones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource": "*"
        }
    ]
}
```

When you register a domain, a hosted zone is created at the same time, so a policy that includes permissions to register domains also requires permissions to create hosted zones. (For domain registration, Route 53 doesn't support granting permissions to individual resources.)

For information about permissions that are required to work with private hosted zones, see [Permissions required to use the Amazon Route 53 console \(p. 580\)](#).

Example 4: Allow creation of inbound and outbound Route 53 Resolver endpoints

The following permissions policy allows users to use the Route 53 console to create Resolver inbound and outbound endpoints.

Some of these permissions are required only to create endpoints in the console. You can omit these permissions if you want to grant permissions only to create inbound and outbound endpoints programmatically:

- `route53resolver>ListResolverEndpoints` lets users see the list of inbound or outbound endpoints so they can verify that an endpoint was created.
- `DescribeAvailabilityZones` is required to display a list of Availability Zones.
- `DescribeVpcs` is required to display a list of VPCs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "route53resolver>CreateResolverEndpoint",
                "route53resolver>ListResolverEndpoints",
                "ec2>CreateNetworkInterface",
                "ec2>CreateNetworkInterfacePermission",
                "ec2:AssociateNetworkInterface"
            ],
            "Resource": "*"
        }
    ]
}
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
    ],
    "Resource": "*"
}
]
```

Using Service-Linked Roles for Amazon Route 53 Resolver

Route 53 Resolver uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Resolver. Service-linked roles are predefined by Resolver and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Resolver easier because you don't have to manually add the necessary permissions. Resolver defines the permissions of its service-linked roles, and unless defined otherwise, only Resolver can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting the related resources. This protects your Resolver resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see [AWS Services that Work with IAM](#) and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Topics

- [Service-Linked Role Permissions for Resolver \(p. 587\)](#)
- [Creating a Service-Linked Role for Resolver \(p. 588\)](#)
- [Editing a Service-Linked Role for Resolver \(p. 588\)](#)
- [Deleting a Service-Linked Role for Resolver \(p. 588\)](#)
- [Supported Regions for Resolver Service-Linked Roles \(p. 589\)](#)

Service-Linked Role Permissions for Resolver

Resolver uses the **AWSServiceRoleForRoute53Resolver** service-linked role to deliver query logs on your behalf.

The role permissions policy allows Resolver to complete the following actions on your resources:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "logs>CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs>UpdateLogDelivery",
                "logs>DeleteLogDelivery",
                "logs>ListLogDeliveries",
                "logs>PutLogDelivery"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

```
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-Linked Role Permissions](#) in the *IAM User Guide*.

Creating a Service-Linked Role for Resolver

You don't need to manually create a service-linked role. When you create a resolver query log configuration association in the Amazon Route 53 console, the AWS CLI, or the AWS API, Resolver creates the service-linked role for you.

Important

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. Also, if you were using the Resolver service before August 12, 2020, when it began supporting service-linked roles, then Resolver created the `AWSServiceRoleForRoute53Resolver` role in your account. To learn more, see [A New Role Appeared in My IAM Account](#).

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a new Resolver query log configuration association, the `AWSServiceRoleForRoute53Resolver` service-linked role is created for you again.

Editing a Service-Linked Role for Resolver

Resolver does not allow you to edit the `AWSServiceRoleForRoute53Resolver` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a Service-Linked Role](#) in the *IAM User Guide*.

Deleting a Service-Linked Role for Resolver

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note

If the Resolver service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete Resolver resources used by the `AWSServiceRoleForRoute53Resolver`

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Expand the Route 53 console menu. In the upper left corner of the console, choose the three horizontal bars (≡) icon.
3. Within the **Resolver** menu, choose **Query logging**.

4. Select the check box next to the name of your query logging configuration, and then choose **Delete**.
5. In the **Delete query logging configuration** text box, select **Stop logging queries**.

This will disassociate the configuration from the VPC. You can also disassociate the query logging configuration programmatically. For more information, see [disassociate-resolver-query-log-config](#).

6. After logging queries has stopped, you can optionally type **delete** in the field and choose **Delete** to delete the query logging configuration. However, this is not necessary for deleting the resources used by `AWSServiceRoleForRoute53Resolver`.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForRoute53Resolver` service-linked role. For more information, see [Deleting a Service-Linked Role](#) in the *IAM User Guide*.

Supported Regions for Resolver Service-Linked Roles

Resolver does not support using service-linked roles in every Region where the service is available. You can use the `AWSServiceRoleForRoute53Resolver` role in the following Regions.

Region name	Region identity	Support in Resolver
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	Yes
US West (N. California)	us-west-1	Yes
US West (Oregon)	us-west-2	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka)	ap-northeast-3	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	Yes
Europe (Frankfurt)	eu-central-1	Yes
Europe (Ireland)	eu-west-1	Yes
Europe (London)	eu-west-2	Yes
Europe (Paris)	eu-west-3	Yes
South America (São Paulo)	sa-east-1	Yes
China (Beijing)	cn-north-1	Yes
China (Ningxia)	cn-northwest-1	Yes
AWS GovCloud (US)	us-gov-east-1	Yes

Region name	Region identity	Support in Resolver
AWS GovCloud (US)	us-gov-west-1	Yes

AWS managed policies for Amazon Route 53

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to [create IAM customer managed policies](#) that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](#) in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ViewOnlyAccess** AWS managed policy provides read-only access to many AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](#) in the *IAM User Guide*.

AWS managed policy: AmazonRoute53FullAccess

You can attach the `AmazonRoute53FullAccess` policy to your IAM identities.

This policy grants full access to Route 53 resources, including domain registration and health checking, but excluding Resolver.

Permissions details

This policy includes the following permissions.

- `route53:*` – Lets you perform all Route 53 actions *except* the following:
 - Create and update alias records for which the value of **Alias Target** is a CloudFront distribution, an Elastic Load Balancing load balancer, an Elastic Beanstalk environment, or an Amazon S3 bucket. (With these permissions, you can create alias records for which the value of **Alias Target** is another record in the same hosted zone.)
 - Work with private hosted zones.
 - Work with domains.
 - Create, delete, and view CloudWatch alarms.
 - Render CloudWatch metrics in the Route 53 console.
- `route53domains:*`– Lets you work with domains.
- `cloudfront>ListDistributions` – Lets you create and update alias records for which the value of **Alias Target** is a CloudFront distribution.

This permission isn't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of distributions to display in the console.

- `elasticloadbalancing:DescribeLoadBalancers` – Lets you create and update alias records for which the value of **Alias Target** is an Elastic Load Balancing load balancer.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of load balancers to display in the console.

- `elasticbeanstalk:DescribeEnvironments` – Lets you create and update alias records for which the value of **Alias Target** is an Elastic Beanstalk environment.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of environments to display in the console.

- `s3>ListBucket`, `s3:GetBucketLocation`, and `s3:GetBucketWebsite` – Let you create and update alias records for which the value of **Alias Target** is an Amazon S3 bucket. (You can create an alias to an Amazon S3 bucket only if the bucket is configured as a website endpoint; `s3:GetBucketWebsite` gets the required configuration information.)

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses these only to get a list of buckets to display in the console.

- `ec2:DescribeVpcs` – Lets you display a list of VPCs.
- `ec2:DescribeVpcEndpoints` – Lets you display a list of VPC endpoints.
- `ec2:DescribeRegions` – Lets you display a list of Availability Zones.
- `sns>ListTopics`, `sns>ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` – Let you create, delete, and view CloudWatch alarms.
- `cloudwatch:GetMetricStatistics` – Lets you create CloudWatch metric health checks.

These permissions aren't required if you aren't using the Route 53 console. Route 53 uses it only to get statistics to display in the console.

- `apigateway:GET` – Lets you create and update alias records for which the value of **Alias Target** is an Amazon API Gateway API.

This permission isn't required if you aren't using the Route 53 console. Route 53 uses it only to get a list of APIs to display in the console.

For more information about the permissions, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#),

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "route53:*",  
                "route53domains:*",  
                "cloudfront>ListDistributions",  
                "elasticloadbalancing:DescribeLoadBalancers",  
                "elasticbeanstalk:DescribeEnvironments",  
                "s3>ListBucket",  
                "s3:GetBucketLocation",  
                "s3:GetBucketWebsite",  
                "ec2:DescribeVpcs",  
                "ec2:DescribeVpcEndpoints",  
                "ec2:DescribeRegions",  
                "sns>ListTopics",  
                "sns>ListSubscriptionsByTopic",  
                "cloudwatch:DescribeAlarms",  
                "cloudwatch:GetMetricStatistics"  
            ],  
            "Resource": "*"  
        },  
        {  
    ]}
```

```
        "Effect": "Allow",
        "Action": "apigateway:GET",
        "Resource": "arn:aws:apigateway:*:::/domainnames"
    }
]
```

AWS managed policy: AmazonRoute53ReadOnlyAccess

You can attach the `AmazonRoute53ReadOnlyAccess` policy to your IAM identities.

This policy grants read-only access to Route 53 resources, including domain registration and health checking, but excluding Resolver.

Permissions details

This policy includes the following permissions.

- `route53:Get*` – Gets the Route 53 resources.
- `route53>List*` – Lists the Route 53 resources.
- `route53:TestDNSAnswer` – Gets the value that Route 53 returns in response to a DNS request.

For more information about the permissions, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#),

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53>List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS managed policy: AmazonRoute53DomainsFullAccess

You can attach the `AmazonRoute53DomainsFullAccess` policy to your IAM identities.

This policy grants full access to Route 53 domain registration resources.

Permissions details

This policy includes the following permissions.

- `route53>CreateHostedZone` – Lets you create a Route 53 hosted zone.
- `route53domains:*` – Lets you register domain names and perform related operations.

For more information about the permissions, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#),

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "route53>CreateHostedZone",  
                "route53domains:*"  
            ],  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

AWS managed policy: AmazonRoute53DomainsReadOnlyAccess

You can attach the `AmazonRoute53DomainsReadOnlyAccess` policy to your IAM identities.

This policy grants read-only access to Route 53 domain registration resources.

Permissions details

This policy includes the following permissions.

- `route53domains:Get*` – Lets you retrieve a list of domains from Route 53.
- `route53domains>List*` – Lets you display a list of Route 53 domains.

For more information about the permissions, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#),

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "route53domains:Get*",  
                "route53domains>List*"  
            ],  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

AWS managed policy: AmazonRoute53ResolverFullAccess

You can attach the `AmazonRoute53ResolverFullAccess` policy to your IAM identities.

This policy grants full access to Route 53 Resolver resources.

Permissions details

This policy includes the following permissions.

- `route53resolver:*` – Lets you create and manage Resolver resources on the Route 53 console.

- `ec2:DescribeSubnets` – Lets you list your Amazon VPC subnets.
- `ec2:CreateNetworkInterface`, `ec2:DeleteNetworkInterface`, and `ec2:ModifyNetworkInterfaceAttribute` – Let you create, modify, and delete network interfaces.
- `ec2:DescribeNetworkInterfaces` – Lets you display a list of network interfaces.
- `ec2:DescribeSecurityGroups` – Lets you display a list of all of your security groups.
- `ec2:DescribeVpcs` – Lets you display a list of VPCs.
- `ec2:DescribeAvailabilityZones` – Lets you list the zones that are available to you.

For more information about the permissions, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#),

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "route53resolver:*",  
                "ec2:DescribeSubnets",  
                "ec2:CreateNetworkInterface",  
                "ec2:DeleteNetworkInterface",  
                "ec2:ModifyNetworkInterfaceAttribute",  
                "ec2:DescribeNetworkInterfaces",  
                "ec2:CreateNetworkInterfacePermission",  
                "ec2:DescribeSecurityGroups",  
                "ec2:DescribeVpcs",  
                "ec2:DescribeAvailabilityZones"  
            ],  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

AWS managed policy: `AmazonRoute53ResolverReadOnlyAccess`

You can attach the `AmazonRoute53ResolverReadOnlyAccess` policy to your IAM identities.

This policy grants read-only access to Route 53 Resolver resources.

Permissions details

This policy includes the following permissions.

- `route53resolver:Get*` – Lets you retrieve list of Resolver resources.
- `route53resolver>List*` – Lets you display a list of Resolver resources.
- `ec2:DescribeNetworkInterfaces` – Lets you display a list of network interfaces.
- `ec2:DescribeSecurityGroups` – Lets you display a list of all of your security groups.

For more information about the permissions, see [Amazon Route 53 API permissions: Actions, resources, and conditions reference \(p. 595\)](#),

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
{
    "Effect": "Allow",
    "Action": [
        "route53resolver:Get*",
        "route53resolver>List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
    ],
    "Resource": [
        "*"
    ]
}
]
```

AWS managed policy: Route53ResolverServiceRolePolicy

You can't attach `Route53ResolverServiceRolePolicy` to your IAM entities. This policy is attached to a service-linked role that allows Route 53 Resolver to access AWS services and resources that are used or managed by Resolver. For more information, see [Using Service-Linked Roles for Amazon Route 53 Resolver \(p. 587\)](#).

Route 53 updates to AWS managed policies

View details about updates to AWS managed policies for Route 53 since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the [Route 53 Document history page \(p. 681\)](#).

Change	Description	Date
Route 53 started tracking changes	Route 53 started tracking changes for its AWS managed policies.	July 14, 2021

Amazon Route 53 API permissions: Actions, resources, and conditions reference

When you set up [Access control \(p. 575\)](#) and write a permissions policy that you can attach to an IAM identity (identity-based policies), you can use the following lists as a reference. The lists include each Amazon Route 53 API action, the actions that you must grant permissions access to, and the AWS resource that you must grant access to. You specify the actions in the policy's `Action` field, and you specify the resource value in the policy's `Resource` field.

You can use AWS-wide condition keys in your Route 53 policies to express conditions. For a complete list of AWS-wide keys, see [Available keys](#) in the *IAM User Guide*.

Note

When granting access, the hosted zone and the Amazon VPC must belong to the same partition. A partition is a group of AWS Regions. Each AWS account is scoped to one partition. The following are the supported partitions:

- aws - AWS Regions
- aws-cn - China Regions

- `aws-us-gov` - AWS GovCloud (US) Region

For more information, see [Access Management](#) in the *AWS General Reference*.

Note

To specify an action, use the applicable prefix (`route53`, `route53domains`, or `route53resolver`) followed by the API operation name, for example:

- `route53:CreateHostedZone`
- `route53domains:RegisterDomain`
- `route53resolver>CreateResolverEndpoint`

Topics

- [Required permissions for actions on public hosted zones \(p. 596\)](#)
- [Required permissions for actions on private hosted zones \(p. 597\)](#)
- [Required permissions for actions on reusable delegation sets \(p. 598\)](#)
- [Required permissions for actions on records \(p. 598\)](#)
- [Required permissions for actions on traffic policies \(p. 599\)](#)
- [Required permissions for actions on traffic policy instances \(p. 600\)](#)
- [Required permissions for actions on health checks \(p. 600\)](#)
- [Required permissions for actions on domain registrations \(p. 601\)](#)
- [Required permissions for Route 53 Resolver actions \(p. 604\)](#)
- [Required permissions for Route 53 Resolver DNS Firewall actions \(p. 607\)](#)
- [Required permissions for actions to get limits for accounts, hosted zones, and reusable delegation sets \(p. 610\)](#)
- [Required permissions for actions on tags for hosted zones and health checks \(p. 610\)](#)
- [Required permissions for actions on tags for domains \(p. 611\)](#)
- [Required permissions for DNSSEC actions \(p. 611\)](#)

Required permissions for actions on public hosted zones

[CreateHostedZone](#)

Required Permissions (API Action): `route53:CreateHostedZone`

Resources: *

[DeleteHostedZone](#)

Required Permissions (API Action): `route53>DeleteHostedZone`

Resources: *

[GetHostedZone](#)

Required Permissions (API Action): `route53:GetHostedZone`

Resources: *

[GetHostedZoneCount](#)

Required Permissions (API Action): `route53:GetHostedZoneCount`

Resources: *

[ListHostedZones](#)

Required Permissions (API Action): `route53>ListHostedZones`

Resources: *

[ListHostedZonesByName](#)

Required Permissions (API Action): `route53>ListHostedZonesByName`

Resources: *

[UpdateHostedZoneComment](#)

Required Permissions (API Action): `route53>UpdateHostedZoneComment`

Resources: *

Required permissions for actions on private hosted zones

[CreateHostedZone](#)

Required Permissions (API Action): `route53>CreateHostedZone`, `ec2>DescribeVpcs`, `ec2>DescribeRegions`

Resources: *, `arn:aws:ec2::optional account id:*`

[DeleteHostedZone](#)

Required Permissions (API Action): `route53>DeleteHostedZone`

Resources: *

[AssociateVPCWithHostedZone](#)

Required Permissions (API Action): `route53>AssociateVPCWithHostedZone`, `ec2>DescribeVpcs`

Resources: *, `arn:aws:ec2::optional account id:*`

[CreateVPCAssociationAuthorization](#)

Required Permissions (API Action): `route53>CreateVPCAssociationAuthorization`

Resources: *

[DeleteVPCAssociationAuthorization](#)

Required Permissions (API Action): `route53>DeleteVPCAssociationAuthorization`

Resources: *

[DisassociateVPCFromHostedZone](#)

Required Permissions (API Action): `route53>DisassociateVPCFromHostedZone`, `ec2>DescribeVpcs`

Resources: *, `arn:aws:ec2::optional account id:*`

[GetHostedZone](#)

Required Permissions (API Action): `route53>GetHostedZone`

Resources: *

[GetHostedZoneCount](#)

Required Permissions (API Action): `route53:GetHostedZoneCount`

Resources: *

[ListHostedZones](#)

Required Permissions (API Action): `route53>ListHostedZones`

Resources: *

[ListHostedZonesByName](#)

Required Permissions (API Action): `route53>ListHostedZonesByName`

Resources: *

[UpdateHostedZoneComment](#)

Required Permissions (API Action): `route53:UpdateHostedZoneComment`

Resources: *

Required permissions for actions on reusable delegation sets

[CreateReusableDelegationSet](#)

Required Permissions (API Action): `route53>CreateReusableDelegationSet`

Resources: *

[DeleteReusableDelegationSet](#)

Required Permissions (API Action): `route53>DeleteReusableDelegationSet`

Resources: *

[GetReusableDelegationSet](#)

Required Permissions (API Action): `route53:GetReusableDelegationSet`

Resources: *

[ListReusableDelegationSets](#)

Required Permissions (API Action): `route53>ListReusableDelegationSets`

Resources: *

Required permissions for actions on records

[ChangeResourceRecordSets](#)

Required Permissions (API Action): `route53:ChangeResourceRecordSets`

Resources: `arn:aws:route53:::hostedzone/hosted zone ID`

[GetChange](#)

Required Permissions (API Action): `route53:GetChange`

Resources: *

[GetGeoLocation](#)

Required Permissions (API Action): None

Resources: None

Route 53 does not perform authorization for this API because it retrieves information that is already available to the public.

[ListGeoLocations](#)

Required Permissions (API Action): None

Resources: None

Route 53 does not perform authorization for this API because it retrieves information that is already available to the public.

[ListResourceRecordSets](#)

Required Permissions (API Action): `route53>ListResourceRecordSets`

Resources: `arn:aws:route53:::hostedzone/hosted zone ID`

Required permissions for actions on traffic policies

[CreateTrafficPolicy](#)

Required Permissions (API Action): `route53>CreateTrafficPolicy`

Resources: *

[CreateTrafficPolicyVersion](#)

Required Permissions (API Action): `route53>CreateTrafficPolicyVersion`

Resources: *

[DeleteTrafficPolicy](#)

Required Permissions (API Action): `route53>DeleteTrafficPolicy`

Resources: *

[GetTrafficPolicy](#)

Required Permissions (API Action): `route53:GetTrafficPolicy`

Resources: *

[ListTrafficPolicies](#)

Required Permissions (API Action): `route53>ListTrafficPolicies`

Resources: *

[ListTrafficPolicyVersions](#)

Required Permissions (API Action): `route53>ListTrafficPolicyVersions`

Resources: *

[UpdateTrafficPolicyComment](#)

Required Permissions (API Action): `route53:UpdateTrafficPolicyComment`

Resources: *

Required permissions for actions on traffic policy instances

[CreateTrafficPolicyInstance](#)

Required Permissions (API Action): `route53:CreateTrafficPolicyInstance`

Resources: *

[DeleteTrafficPolicyInstance](#)

Required Permissions (API Action): `route53>DeleteTrafficPolicyInstance`

Resources: *

[GetTrafficPolicyInstance](#)

Required Permissions (API Action): `route53:GetTrafficPolicyInstance`

Resources: *

[GetTrafficPolicyInstanceCount](#)

Required Permissions (API Action): `route53:GetTrafficPolicyInstanceCount`

Resources: *

[ListTrafficPolicyInstances](#)

Required Permissions (API Action): `route53>ListTrafficPolicyInstances`

Resources: *

[ListTrafficPolicyInstancesByHostedZone](#)

Required Permissions (API Action): `route53>ListTrafficPolicyInstancesByHostedZone`

Resources: *

[ListTrafficPolicyInstancesByPolicy](#)

Required Permissions (API Action): `route53>ListTrafficPolicyInstancesByPolicy`

Resources: *

[UpdateTrafficPolicyInstance](#)

Required Permissions (API Action): `route53:UpdateTrafficPolicyInstance`

Resources: *

Required permissions for actions on health checks

[CreateHealthCheck](#)

Required Permissions (API Action): `route53>CreateHealthCheck`

Resources: *

[DeleteHealthCheck](#)

Required Permissions (API Action): `route53>DeleteHealthCheck`

Resources: *, `arn:aws:route53:::healthcheck/health check ID`

[GetCheckerIpRanges](#)

Required Permissions (API Action): None

Resources: *

Route 53 does not perform authorization for this API because it retrieves information that is already available to the public.

[GetHealthCheck](#)

Required Permissions (API Action): `route53:GetHealthCheck`

Resources: *, `arn:aws:route53:::healthcheck/health check ID`

[GetHealthCheckCount](#)

Required Permissions (API Action): `route53:GetHealthCheckCount`

Resources: *

[GetHealthCheckLastFailureReason](#)

Required Permissions (API Action): `route53:GetHealthCheckLastFailureReason`

Resources: *, `arn:aws:route53:::healthcheck/health check ID`

[GetHealthCheckStatus](#)

Required Permissions (API Action): `route53:GetHealthCheckStatus`

Resources: *, `arn:aws:route53:::healthcheck/health check ID`

[ListHealthChecks](#)

Required Permissions (API Action): `route53>ListHealthChecks`

Resources: *

[UpdateHealthCheck](#)

Required Permissions (API Action): `route53:UpdateHealthCheck`

Resources: *, `arn:aws:route53:::healthcheck/health check ID`

Required permissions for actions on domain registrations

[AcceptDomainTransferFromAnotherAwsAccount](#)

Required Permissions (API Action):

`route53domains:AcceptDomainTransferFromAnotherAwsAccount`

Resources: *

[AddDnssec \(console only\)](#)

Required Permissions (API Action): `route53domains:AddDnssec`

Resources: *

[CancelDomainTransferToAnotherAwsAccount](#)

Required Permissions (API Action):

`route53domains:CancelDomainTransferToAnotherAwsAccount`

Resources: *

[CheckDomainAvailability](#)

Required Permissions (API Action): `route53domains:CheckDomainAvailability`

Resources: *

[CheckDomainTransferability](#)

Required Permissions (API Action): `route53domains:CheckDomainTransferability`

Resources: *

[DeleteDomain](#) (console only)

Required Permissions (API Action): `route53domains>DeleteDomain`

Resources: *

[DisableDomainAutoRenew](#)

Required Permissions (API Action): `route53domains:ChangeAutoRenew`

Resources: *

[DisableDomainTransferLock](#)

Required Permissions (API Action): `route53domains:DisableDomainTransferLock`

Resources: *

[EnableDomainAutoRenew](#)

Required Permissions (API Action): `route53domains:ChangeAutoRenew`

Resources: *

[EnableDomainTransferLock](#)

Required Permissions (API Action): `route53domains:EnableDomainTransferLock`

Resources: *

[GetContactReachabilityStatus](#)

Required Permissions (API Action): `route53domains>ListDomains`

Resources: *

[GetDomainDetail](#)

Required Permissions (API Action): `route53domains:GetDomainDetail`

Resources: *

[GetDomainSuggestions](#)

Required Permissions (API Action): `route53domains>ListDomains`

Resources: *

[GetOperationDetail](#)

Required Permissions (API Action): `route53domains:GetOperationDetail`

Resources: *

[ListDnssec](#) (console only)

Required Permissions (API Action): `route53domains>ListDnssec`

Resources: *

[ListDomains](#)

Required Permissions (API Action): `route53domains>ListDomains`

Resources: *

[ListOperations](#)

Required Permissions (API Action): `route53domains>ListOperations`

Resources: *

[RegisterDomain](#)

Required Permissions (API Action): `route53domains/RegisterDomain`

Resources: *

[RejectDomainTransferFromAnotherAwsAccount](#)

Required Permissions (API Action):

`route53domains RejectDomainTransferFromAnotherAwsAccount`

Resources: *

[RemoveDnssec](#) (console only)

Required Permissions (API Action): `route53domains RemoveDnssec`

Resources: *

[RenewDomain](#)

Required Permissions (API Action): `route53domains RegisterDomain`

Resources: *

[ResendContactReachabilityEmail](#)

Required Permissions (API Action): `route53domains ListDomains`

Resources: *

[RetrieveDomainAuthCode](#)

Required Permissions (API Action): `route53domains RetrieveDomainAuthCode`

Resources: *

[TransferDomain](#)

Required Permissions (API Action): `route53domains TransferDomain`

Resources: *

[TransferDomainToAnotherAwsAccount](#)

Required Permissions (API Action): `route53domains TransferDomainToAnotherAwsAccount`

Resources: *

[UpdateDomainContact](#)

Required Permissions (API Action): `route53domains UpdateDomainContact`

Resources: *

[UpdateDomainContactPrivacy](#)

Required Permissions (API Action): `route53domains:UpdateDomainContactPrivacy`

Resources: *

[UpdateDomainNameservers](#)

Required Permissions (API Action): `route53domains:UpdateDomainNameservers`

Resources: *

[ViewBilling](#)

Required Permissions (API Action): `route53domains:ViewBilling`

Resources: *

Required permissions for Route 53 Resolver actions

[AssociateResolverEndpointIpAddress](#)

Required Permissions (API Action):

`route53resolver:AssociateResolverEndpointIpAddress,`
`ec2:CreateNetworkInterfacePermission, ec2:DescribeAvailabilityZones,`
`ec2:DescribeNetworkInterfaces, ec2:DescribeSubnets`

Resources: *

[AssociateResolverQueryLogConfig](#)

Required Permissions (API Action): `route53resolver:AssociateResolverQueryLogConfig,`
`logs:DescribeResourcePolicies, logs:DescribeLogGroups, logs:GetLogDelivery,`
`logs>ListLogDeliveries, logs:PutResourcePolicy, logs:UpdateLogDelivery`

Resources: *

[AssociateResolverRule](#)

Required Permissions (API Action): `route53resolver:AssociateResolverRule,`
`ec2:DescribeVpcs`

Resources: *

[CreateResolverEndpoint](#)

Required Permissions (API Action): `route53resolver>CreateResolverEndpoint,`
`ec2:DescribeSubnets, ec2:CreateNetworkInterface, ec2:DescribeNetworkInterfaces,`
`ec2:CreateNetworkInterfacePermission, ec2:DescribeSecurityGroups`

See also [Example 4: Allow creation of inbound and outbound Route 53 Resolver endpoints \(p. 586\)](#).

Resources: *

[CreateResolverQueryLogConfig](#)

Required Permissions (API Action): `route53resolver>CreateResolverQueryLogConfig,`
`ec2:DescribeVpcs, logs:DescribeResourcePolicies, logs:DescribeLogGroups,`
`logs>CreateLogDelivery, logs>DeleteLogDelivery logs:GetLogDelivery,`
`logs>ListLogDeliveries, logs:UpdateLogDelivery, iam>CreateServiceLinkedRole`

Resources: *

[CreateResolverRule](#)

Required Permissions (API Action): `route53resolver:CreateResolverRule`

Resources: *

[DeleteResolverEndpoint](#)

Required Permissions (API Action): `route53resolver:DeleteResolverEndpoint`,
`ec2:DeleteNetworkInterface`, `ec2:DescribeNetworkInterface`

Resources: *

[DeleteResolverQueryLogConfig](#)

Required Permissions (API Action): `route53resolver:DeleteResolverQueryLogConfig`,
`logs:DescribeResourcePolicies`, `logs:DescribeLogGroups`, `logs:DeleteLogDelivery`
`logs:GetLogDelivery`, `logs>ListLogDeliveries`, `logs:UpdateLogDelivery`

Resources: *

[DeleteResolverRule](#)

Required Permissions (API Action): `route53resolver:DeleteResolverRule`

Resources: *

[DisassociateResolverEndpointIpAddress](#)

Required Permissions (API Action):
`route53resolver:DisassociateResolverEndpointIpAddress`,
`ec2:DeleteNetworkInterface`

Resources: *

[DisassociateResolverQueryLogConfig](#)

Required Permissions (API Action):
`route53resolver:DisassociateResolverQueryLogConfig`,
`logs:DescribeResourcePolicies`, `logs:DescribeLogGroups`, `logs:GetLogDelivery`,
`logs>ListLogDeliveries`, `logs:PutResourcePolicy`, `logs:UpdateLogDelivery`

Resources: *

[DisassociateResolverRule](#)

Required Permissions (API Action): `route53resolver:DisassociateResolverRule`

Resources: *

[GetResolverEndpoint](#)

Required Permissions (API Action): `route53resolver:GetResolverEndpoint`

Resources: *

[GetResolverQueryLogConfig](#)

Required Permissions (API Action): `route53resolver:GetResolverQueryLogConfig`,
`logs:DescribeResourcePolicies`, `logs:DescribeLogGroups`, `logs:GetLogDelivery`,
`logs>ListLogDeliveries`

Resources: *

[GetResolverQueryLogConfigAssociation](#)

Required Permissions (API Action):
`route53resolver:GetResolverQueryLogConfigAssociation`,

logs:DescribeResourcePolicies, logs:DescribeLogGroups, logs:GetLogDelivery,
logs>ListLogDeliveries

Resources: *

[GetResolverQueryLogConfigPolicy](#)

Required Permissions (API Action): route53resolver:GetResolverQueryLogConfigPolicy,
logs:DescribeResourcePolicies, logs:DescribeLogGroups, logs:GetLogDelivery,
logs>ListLogDeliveries

Resources: *

[GetResolverRule](#)

Required Permissions (API Action): route53resolver:GetResolverRule

Resources: *

[GetResolverRuleAssociation](#)

Required Permissions (API Action): route53resolver:GetResolverRuleAssociation,
ec2:DescribeVpcs

Resources: *

[GetResolverRulePolicy](#)

Required Permissions (API Action): route53resolver:GetResolverRulePolicy

Resources: *

[ListResolverEndpointIpAddresses](#)

Required Permissions (API Action): route53resolver>ListResolverEndpointIpAddresses

Resources: *

[ListResolverEndpoints](#)

Required Permissions (API Action): route53resolver>ListResolverEndpoints

Resources: *

[ListResolverQueryLogConfigAssociations](#)

Required Permissions (API Action):
route53resolver>ListResolverQueryLogConfigAssociations,
logs:DescribeResourcePolicies, logs:DescribeLogGroups, logs:GetLogDelivery,
logs>ListLogDeliveries

Resources: *

[ListResolverQueryLogConfigs](#)

Required Permissions (API Action): route53resolver>ListResolverQueryLogConfigs,
logs:DescribeResourcePolicies, logs:DescribeLogGroups, logs:GetLogDelivery,
logs>ListLogDeliveries

Resources: *

[ListResolverRuleAssociations](#)

Required Permissions (API Action): route53resolver>ListResolverRuleAssociations,
ec2:DescribeVpcs

Resources: *

[ListResolverRules](#)

Required Permissions (API Action): `route53resolver>ListResolverRules`

Resources: *

[ListTagsForResource](#)

Required Permissions (API Action): `route53resolver>ListTagsForResource`

Resources: `arn:aws:route53resolver:::resolver-endpoint/*,`
`arn:aws:route53resolver:::resolver-rule/`

[PutResolverQueryLogConfigPolicy](#)

Required Permissions (API Action): `route53resolverPutResolverQueryLogConfigPolicy`,
`logs:DescribeResourcePolicies`, `logs:DescribeLogGroups`, `logs:GetLogDelivery`,
`logs>ListLogDeliveries`, `logs:PutResourcePolicy`, `logs:UpdateLogDelivery`

Resources: *

[PutResolverRulePolicy](#)

Required Permissions (API Action): `route53resolverPutResolverRulePolicy`

Resources: *

[TagResource](#)

Required Permissions (API Action): `route53resolverTagResource`

Resources: `arn:aws:route53resolver:::resolver-endpoint/*,`
`arn:aws:route53resolver:::resolver-rule/*`

[UntagResource](#)

Required Permissions (API Action): `route53resolverUntagResource`

Resources: `arn:aws:route53resolver:::resolver-endpoint/*,`
`arn:aws:route53resolver:::resolver-rule/*`

[UpdateResolverEndpoint](#)

Required Permissions (API Action): `route53resolverUpdateResolverEndpoint`

Resources: *

[UpdateResolverRule](#)

Required Permissions (API Action): `route53resolverUpdateResolverRule`

Resources: *

Required permissions for Route 53 Resolver DNS Firewall actions

[AssociateFirewallRuleGroup](#)

Required Permissions (API Action): `route53resolverAssociateFirewallRuleGroup`,
`ec2DescribeVpcs`

Optional Permissions: `route53resolverTagResource` (Required if you provide a tagging parameter)

Resources: *

[CreateFirewallDomainList](#)

Required Permissions (API Action): `route53resolver:CreateFirewallDomainList`

Optional Permissions: `route53resolver:TagResource` (Required if you provide a tagging parameter)

Resources: *

[CreateFirewallRule](#)

Required Permissions (API Action): `route53resolver:CreateFirewallRule`

Resources: *

[CreateFirewallRuleGroup](#)

Required Permissions (API Action): `route53resolver:CreateFirewallRuleGroup`

Optional Permissions: `route53resolver:TagResource` (Required if you provide a tagging parameter)

Resources: *

[DeleteFirewallDomainList](#)

Required Permissions (API Action): `route53resolver:DeleteFirewallDomainList`

Resources: *

[DeleteFirewallRule](#)

Required Permissions (API Action): `route53resolver:DeleteFirewallRule`

Resources: *

[DeleteFirewallRuleGroup](#)

Required Permissions (API Action): `route53resolver:DeleteFirewallRuleGroup`

Resources: *

[DisassociateFirewallRuleGroup](#)

Required Permissions (API Action): `route53resolver:DisassociateFirewallRuleGroup`

Resources: *

[GetFirewallConfig](#)

Required Permissions (API Action): `route53resolver:GetFirewallConfig ec2:DescribeVpcs`

Resources: *

[GetFirewallDomainList](#)

Required Permissions (API Action): `route53resolver:GetFirewallDomainList`

Resources: *

[GetFirewallRuleGroup](#)

Required Permissions (API Action): `route53resolver:GetFirewallRuleGroup`

Resources: *

[GetFirewallRuleGroupAssociation](#)

Required Permissions (API Action): `route53resolver:GetFirewallRuleGroupAssociation`

Resources: *

[GetFirewallRuleGroupPolicy](#)

Required Permissions (API Action): `route53resolver:GetFirewallRuleGroupPolicy`

Resources: *

[ImportFirewallDomains](#)

Required Permissions (API Action): `route53resolver:ImportFirewallRuleDomains`

Resources: *

[ListFirewallConfigs](#)

Required Permissions (API Action): `route53resolver>ListFirewallConfigs`
`ec2:DescribeVpcs`

Resources: *

[ListFirewallDomainLists](#)

Required Permissions (API Action): `route53resolver>ListFirewallDomainLists`

Resources: *

[ListFirewallDomains](#)

Required Permissions (API Action): `route53resolver>ListFirewallDomains`

Resources: *

[ListFirewallRuleGroupAssociations](#)

Required Permissions (API Action): `route53resolver>ListFirewallRuleGroupAssociations`

Resources: *

[ListFirewallRuleGroups](#)

Required Permissions (API Action): `route53resolver>ListFirewallRuleGroups`

Resources: *

[ListFirewallRules](#)

Required Permissions (API Action): `route53resolver>ListFirewallRules`

Resources: *

[PutFirewallRuleGroupPolicy](#)

Required Permissions (API Action): `route53resolver:PutFirewallRuleGroupPolicy`

Resources: *

[UpdateFirewallConfig](#)

Required Permissions (API Action): `route53resolver:UpdateFirewallConfig`
`ec2:DescribeVpcs`

Resources: *

[UpdateFirewallDomains](#)

Required Permissions (API Action): `route53resolver:UpdateFirewallDomains`

Resources: *

[UpdateFirewallRule](#)

Required Permissions (API Action): `route53resolver:UpdateFirewallRule`

Resources: *

[UpdateFirewallRuleGroupAssociation](#)

Required Permissions (API Action):

`route53resolver:UpdateFirewallRuleGroupAssociation`

Resources: *

Required permissions for actions to get limits for accounts, hosted zones, and reusable delegation sets

[GetAccountLimit](#)

Required Permissions (API Action): `route53:GetAccountLimit`

Resources: *

[GetHostedZoneLimit](#)

Required Permissions (API Action): `route53:GetHostedZoneLimit`

Resources: *

[GetReusableDelegationSetLimit](#)

Required Permissions (API Action): `route53:GetReusableDelegationSetLimit`

Resources: *

Required permissions for actions on tags for hosted zones and health checks

[ChangeTagsForResource](#)

Required Permissions (API Action): `route53:ChangeTagsForResource`

Resources:

- `arn:aws:route53:::healthcheck/*`
- `arn:aws:route53:::hostedzone/*`

[ListTagsForResource](#)

Required Permissions (API Action): `route53>ListTagsForResource`

Resources:

- `arn:aws:route53:::healthcheck/*`
- `arn:aws:route53:::hostedzone/*`

[ListTagsForResources](#)

Required Permissions (API Action): `route53>ListTagsForResources`

Resources:

- `arn:aws:route53:::healthcheck/*`
- `arn:aws:route53:::hostedzone/*`

Required permissions for actions on tags for domains

[DeleteTagsForDomain](#)

Required Permissions (API Action): `route53domains>DeleteTagsForDomain`

Resources: *

[ListTagsForDomain](#)

Required Permissions (API Action): `route53domains>ListTagsForDomain`

Resources: *

[UpdateTagsForDomain](#)

Required Permissions (API Action): `route53domains>UpdateTagsForDomain`

Resources: *

Required permissions for DNSSEC actions

[GetDNSSEC](#)

Required Permissions (API Action): `route53domains>DeleteTagsForDomain`

Resources: *

[CreateKeySigningKey](#)

Required Permissions (API Action): `route53>CreateKeySigningKey, kms:DescribeKey, kms:GetPublicKey, kms:Sign`

Resources: *

[DeleteKeySigningKey](#)

Required Permissions (API Action): `route53>DeleteKeySigningKey, kms:DescribeKey, kms:GetPublicKey, kms:Sign`

Resources: *

[ActivateKeySigningKey](#)

Required Permissions (API Action): `route53>ActivateKeySigningKey, kms:DescribeKey, kms:GetPublicKey, kms:Sign`

Resources: *

[DeactivateKeySigningKey](#)

Required Permissions (API Action): `route53>DeactivateKeySigningKey, kms:DescribeKey, kms:GetPublicKey, kms:Sign`

Resources: *

[EnableHostedZoneDNSSEC](#)

Required Permissions (API Action): `route53:EnableHostedZoneDNSSEC`, `kms:DescribeKey`, `kms:GetPublicKey`, `kms:Sign`

Resources: *

[DisableHostedZoneDNSSEC](#)

Required Permissions (API Action): `route53:DisableHostedZoneDNSSEC`, `kms:DescribeKey`, `kms:GetPublicKey`, `kms:Sign`

Resources: *

Logging and monitoring in Amazon Route 53

Amazon Route 53 provides DNS query logging and the ability to monitor your resources using health checks. In addition, Route 53 integrates with other AWS services to provide additional logging and monitoring:

Logging DNS queries

You can configure Route 53 to log information about the queries that Route 53 receives, such as the domain or subdomain that was requested, the date and time of the request, and the DNS record type, such as A or AAAA.

For more information, see [Public DNS query logging \(p. 615\)](#).

Using AWS CloudTrail to log console and programmatic actions

CloudTrail provides a record of Route 53 actions taken by a user, a role, or an AWS service. Using the information collected by CloudTrail, you can track the requests that are made, the IP addresses that requests originate from, who made the request, when it was made, and additional details. For more information, see [Logging Amazon Route 53 API calls with AWS CloudTrail \(p. 635\)](#).

Monitoring domain registrations

The Route 53 dashboard provides detailed information about the status of your domain registrations, such as the status of domain transfers and domains that are approaching the expiration date.

For more information, see [Monitoring domain registrations \(p. 626\)](#).

Using Route 53 health checks and Amazon CloudWatch to monitor your resources

You can monitor your resources by creating Route 53 health checks, which use CloudWatch to collect and process raw data into readable, near real-time metrics.

For more information, see [Monitoring your resources with Amazon Route 53 health checks and Amazon CloudWatch \(p. 626\)](#).

Using Amazon CloudWatch to monitor Route 53 Resolver endpoints

You can use CloudWatch to monitor the number of DNS queries that are forwarded by Resolver endpoints.

For more information, see [Monitoring Route 53 Resolver endpoints with Amazon CloudWatch \(p. 630\)](#).

Using AWS Trusted Advisor

Trusted Advisor draws upon best practices learned from serving AWS customers. Trusted Advisor inspects your AWS environment and then makes recommendations when opportunities exist to save

money, improve system availability and performance, or help close security gaps. All AWS customers have access to five Trusted Advisor checks. Customers with a Business or Enterprise support plan can view all Trusted Advisor checks.

For more information, see [Trusted Advisor](#).

Compliance validation for Amazon Route 53

Third-party auditors assess the security and compliance of Amazon Route 53 as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](#). For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading reports in AWS Artifact](#).

Your compliance responsibility when using Route 53 is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. If your use of Route 53 is subject to compliance with standards such as HIPAA, PCI, or FedRAMP, AWS provides resources to help:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- [Architecting for HIPAA Security and Compliance Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [AWS Config](#) – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon Route 53

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

Route 53 is primarily a global service, but the following features support AWS Regions:

- If you're using Route 53 Resolver to set up hybrid configurations, you create endpoints in AWS Regions that you choose, and you specify IP addresses in multiple Availability Zones. For outbound endpoints, you create rules in the same Region where you created the endpoint. For more information, see [Resolving DNS queries between VPCs and your network \(p. 471\)](#).
- You can configure Route 53 health checks to check the health of resources that you create in specific Regions, such as Amazon EC2 instances and Elastic Load Balancing load balancers.
- When you create a health check that monitors an endpoint, you can optionally specify the Regions that you want Route 53 to perform health checks from.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

Infrastructure security in Amazon Route 53

As a managed service, Amazon Route 53 is protected by the AWS global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#) whitepaper.

You use AWS published API calls to access Route 53 through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

Monitoring Amazon Route 53

Monitoring is an important part of maintaining the reliability, availability, and performance of your AWS solutions. You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. However, before you start monitoring, you should create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- What resources will you monitor?
- How often will you monitor these resources?
- What monitoring tools will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something goes wrong?

Topics

- [Public DNS query logging \(p. 615\)](#)
- [Resolver query logging \(p. 619\)](#)
- [Monitoring domain registrations \(p. 626\)](#)
- [Monitoring your resources with Amazon Route 53 health checks and Amazon CloudWatch \(p. 626\)](#)
- [Monitoring hosted zones using Amazon CloudWatch \(p. 628\)](#)
- [Monitoring Route 53 Resolver endpoints with Amazon CloudWatch \(p. 630\)](#)
- [Monitoring Route 53 Resolver DNS Firewall rule groups with Amazon CloudWatch \(p. 633\)](#)
- [Logging Amazon Route 53 API calls with AWS CloudTrail \(p. 635\)](#)

Public DNS query logging

You can configure Amazon Route 53 to log information about the public DNS queries that Route 53 receives, such as the following:

- Domain or subdomain that was requested
- Date and time of the request
- DNS record type (such as A or AAAA)
- Route 53 edge location that responded to the DNS query
- DNS response code, such as `NoError` or `ServFail`

Once you configure query logging, Route 53 will send logs to CloudWatch Logs. You use CloudWatch Logs tools to access the query logs.

Note

Query logging is also available for private hosted zones. For more information, see [Resolver query logging \(p. 619\)](#).

Query logs contain only the queries that DNS resolvers forward to Route 53. If a DNS resolver has already cached the response to a query (such as the IP address for a load balancer for example.com), the resolver will continue to return the cached response without forwarding the query to Route 53 until the TTL for the corresponding record expires.

Depending on how many DNS queries are submitted for a domain name (example.com) or subdomain name (www.example.com), which resolvers your users are using, and the TTL for the record, query logs might contain information about only one query out of every several thousand queries that are submitted to DNS resolvers. For more information about how DNS works, see [How internet traffic is routed to your website or web application \(p. 2\)](#).

If you don't need detailed logging information, you can use Amazon CloudWatch metrics to see the total number of DNS queries that Route 53 responds to for a hosted zone. For more information, see [Viewing DNS query metrics for a public hosted zone \(p. 342\)](#).

Topics

- [Configuring logging for DNS queries \(p. 616\)](#)
- [Using Amazon CloudWatch to access DNS query logs \(p. 617\)](#)
- [Changing the retention period for logs and exporting logs to Amazon S3 \(p. 617\)](#)
- [Stopping query logging \(p. 617\)](#)
- [Values that appear in DNS query logs \(p. 618\)](#)
- [Query log example \(p. 619\)](#)

Configuring logging for DNS queries

To start logging DNS queries for a specified hosted zone, you perform the following tasks in the Amazon Route 53 console:

- Choose the CloudWatch Logs log group that you want Route 53 to publish logs to, or create a new log group.

Note

The log group must be in the US East (N. Virginia) Region.

- Choose **Create** to finish.

Note

If users are submitting DNS queries for your domain, you should start to see queries in the logs within several minutes after you create the query logging configuration.

To configure logging for DNS queries

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted zones**.
3. Choose the hosted zone that you want to configure query logging for.
4. In the **Hosted zone details** pane, choose **Configure query logging**.
5. Choose an existing log group or create a new log group.
6. If you receive an alert about permissions (this happens if you haven't configured query logging with the new console before), do one of the following:
 - If you have 10 resource policies already, you can't create any more. Select any of your resource policies, and select **Edit**. Editing will give Route 53 permissions to write logs to your log groups. Choose **Save**. The alert goes away and you can continue to the next step.
 - If you have never configured query logging before (or if you haven't created 10 resource policies already), you need to grant permissions to Route 53 to write logs to your CloudWatch Logs groups. Choose **Grant permissions**. The alert goes away and you can continue to the next step.
7. Choose **Permissions - optional** to see a table that shows whether the resource policy matches the CloudWatch log group, and whether the Route 53 has the permission to publish logs to CloudWatch.

8. Choose **Create**.

Using Amazon CloudWatch to access DNS query logs

Amazon Route 53 sends query logs directly to CloudWatch Logs; the logs are never accessible through Route 53. Instead, you use CloudWatch Logs to view logs in near real-time, search and filter data, and export logs to Amazon S3.

Route 53 creates one CloudWatch Logs log stream for each Route 53 edge location that responds to DNS queries for the specified hosted zone and sends query logs to the applicable log stream. The format for the name of each log stream is *hosted-zone-id/edge-location-ID*, for example, Z1D633PJN98FT9/DFW3.

Each edge location is identified by a three-letter code and an arbitrarily assigned number, for example, DFW3. The three-letter code typically corresponds with the International Air Transport Association airport code for an airport near the edge location. (These abbreviations might change in the future.) For a list of edge locations, see "The Route 53 Global Network" on the [Route 53 Product Details](#) page.

For more information, see the applicable documentation:

- [Amazon CloudWatch Logs User Guide](#)
- [Amazon CloudWatch Logs API Reference](#)
- [CloudWatch Logs section of the AWS CLI Command Reference](#)
- [Values that appear in DNS query logs \(p. 618\)](#)

Changing the retention period for logs and exporting logs to Amazon S3

By default, CloudWatch Logs stores query logs indefinitely. You can optionally specify a retention period so that CloudWatch Logs deletes logs that are older than the retention period. For more information, see [Change log data retention in CloudWatch Logs](#) in the *Amazon CloudWatch User Guide*.

If you want to retain log data but you don't need CloudWatch Logs tools to view and analyze the data, you can export logs to Amazon S3, which can reduce your storage costs. For more information, see [Exporting log data to Amazon S3](#).

For information about pricing, see the applicable pricing page:

- "Amazon CloudWatch Logs" on the [CloudWatch Pricing](#) page
- [Amazon S3 Pricing](#)

Note

When you configure Route 53 to log DNS queries, you don't incur any Route 53 charges.

Stopping query logging

If you want Amazon Route 53 to stop sending query logs to CloudWatch Logs, perform the following procedure to delete the query logging configuration.

To delete a query logging configuration

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

2. In the navigation pane, choose **Hosted zones**.
3. Choose the name for the hosted zone that you want to delete the query logging configuration for.
4. In the **Hosted zone details** pane, choose **Delete query logging configuration**.
5. Choose **Delete** to confirm.

Values that appear in DNS query logs

Each log file contains one log entry for each DNS query that Amazon Route 53 received from DNS resolvers in the corresponding edge location. Each log entry includes the following values:

Log format version

The version number of this query log. If we add fields to the log or change the format of existing fields, we'll increment this value.

Query timestamp

The date and time that Route 53 responded to the request, in ISO 8601 format and Coordinated Universal Time (UTC), for example, 2017-03-16T19:20:25.177Z.

For information about ISO 8601 format, see the Wikipedia article [ISO 8601](#). For information about UTC, see the Wikipedia article [Coordinated Universal Time](#).

Hosted zone ID

The ID of the hosted zone that is associated with all the DNS queries in this log.

Query name

The domain or subdomain that was specified in the request.

Query type

Either the DNS record type that was specified in the request, or ANY. For information about the types that Route 53 supports, see [Supported DNS record types \(p. 382\)](#).

Response code

The DNS response code that Route 53 returned in response to the DNS query.

Layer 4 protocol

The protocol that was used to submit the query, either TCP or UDP.

Route 53 edge location

The Route 53 edge location that responded to the query. Each edge location is identified by a three-letter code and an arbitrary number, for example, DFW3. The three-letter code typically corresponds with the International Air Transport Association airport code for an airport near the edge location. (These abbreviations might change in the future.)

For a list of edge locations, see "The Route 53 Global Network" on the [Route 53 Product Detail](#) page.

Resolver IP address

The IP address of the DNS resolver that submitted the request to Route 53.

EDNS client subnet

A partial IP address for the client that the request originated from, if available from the DNS resolver.

For more information, see the IETF draft [Client Subnet in DNS Requests](#).

Query log example

Here's an example query log (Region is a 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 -
```

Resolver query logging

You can log the following DNS queries:

- Queries that originate in Amazon Virtual Private Cloud VPCs that you specify, as well as the responses to those DNS queries.
- Queries from on-premises resources that use an inbound Resolver endpoint.
- Queries that use an outbound Resolver endpoint for recursive DNS resolution.
- Queries that use Route 53 Resolver DNS Firewall rules to block, allow, or monitor domain lists.

Resolver query logs include values such as the following:

- The AWS Region where the VPC was created
- The ID of the VPC that the query originated from
- The IP address of the instance that the query originated from
- The instance ID of the resource that the query originated from
- The date and time that the query was first made
- The DNS name requested (such as prod.example.com)
- The DNS record type (such as A or AAAA)
- The DNS response code, such as `NoError` or `ServFail`
- The DNS response data, such as the IP address that is returned in response to the DNS query
- A response to a DNS Firewall rule action

For a detailed list of all of the values logged and an example, see [Values that appear in Resolver query logs \(p. 622\)](#).

Note

As is standard for DNS resolvers, resolvers cache DNS queries for a length of time determined by the time-to-live (TTL) for the resolver. The Route 53 Resolver caches queries that originate in your VPCs, and responds from the cache whenever possible to speed up responses. Resolver query logging logs only unique queries, not queries that Resolver is able to respond to from the cache.

For example, suppose that an EC2 instance in one of the VPCs that a query logging configuration is logging queries for, submits a request for accounting.example.com. Resolver

caches the response to that query, and logs the query. If the same instance's elastic network interface makes a query for accounting.example.com within the TTL of the Resolver's cache, Resolver responds to the query from the cache. The second query is not logged.

You can send the logs to one of the following AWS resources:

- Amazon CloudWatch Logs (CloudWatch Logs) log group
- Amazon S3 (S3) bucket
- Kinesis Data Firehose delivery stream

For more information, see [AWS resources that you can send Resolver query logs to \(p. 620\)](#).

Topics

- [AWS resources that you can send Resolver query logs to \(p. 620\)](#)
- [Managing Resolver query logging configurations \(p. 621\)](#)

AWS resources that you can send Resolver query logs to

Note

If you expect to log queries for workloads with high queries per second (QPS), you should use Amazon S3 to ensure your query logs are not throttled when written to your destination.

If you use Amazon CloudWatch, you can increase your requests per second limit for the PutLogEvents operation. To learn more about increasing your CloudWatch limits, see [CloudWatch Logs quotas](#) in the *Amazon CloudWatch User Guide*.

You can send Resolver query logs to the following AWS resources:

Amazon CloudWatch Logs (Amazon CloudWatch Logs) log group

You can analyze logs with Logs Insights and create metrics and alarms.

For more information, see the [Amazon CloudWatch Logs User Guide](#).

Amazon S3 (S3) bucket

An S3 bucket is economical for long-term log archiving. Latency is typically higher.

If you want to send logs to an S3 bucket in an account that you don't own, the owner of the S3 bucket must add permissions for your account in their bucket policy. For example:

```
{  
    "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": {  
                "AWS": "AROAY12345678901234567890:12345678901234567890123456789012"  
            },  
            "Action": "s3:PutObject",  
            "Resource": "arn:aws:s3:::your_bucket_name/AWSLogs/your_caller_account/*"  
        }  
    ]  
}
```

```
        "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

If you want to store logs in a central S3 bucket for your organization, we recommend that you set up your query logging configuration from a centralized account (with the necessary permissions to write to a central bucket) and use [RAM \(p. 624\)](#) to share the configuration across accounts.

For more information, see the [Amazon Simple Storage Service User Guide](#).

Kinesis Data Firehose delivery stream

You can stream logs in real time to Amazon OpenSearch Service, Amazon Redshift, or other applications.

For more information, see the [Amazon Kinesis Data Firehose Developer Guide](#).

For information about the pricing for Resolver query logging, see [Amazon CloudWatch pricing](#).

CloudWatch Logs charges apply when using flow logs, even when logs are published directly to Amazon S3. For more information, see [Deliver Logs to S3 at Amazon CloudWatch pricing](#).

Managing Resolver query logging configurations

Configuring (Resolver query logging)

To start logging DNS queries that originate in your VPCs, you perform the following tasks in the Amazon Route 53 console:

To configure Resolver query logging

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. Expand the Route 53 console menu. In the upper left corner of the console, choose the three horizontal bars (≡) icon.
3. Within the Resolver menu, choose **Query logging**.
4. In the Region selector, choose the AWS Region where you want to create the query logging configuration. This must be the same Region where you created the VPCs that you want to log DNS queries for. If you have VPCs in multiple Regions, you must create at least one query logging configuration for each Region.
5. Choose **Configure query logging**.

6. Specify the following values:

Query logging configuration name

Enter a name for your query logging configuration. The name appears in the console in the list of query logging configurations. Enter a name that will help you find this configuration later.

Query logs destination

Choose the type of AWS resource that you want Resolver to send query logs to. For information about how to choose among the options (CloudWatch Logs log group, S3 bucket, and Kinesis Data Firehose delivery stream), see [AWS resources that you can send Resolver query logs to \(p. 620\)](#).

After you choose the type of resource, you can either create another resource of that type or choose an existing resource that was created by the current AWS account.

Note

You can choose only resources that were created in the AWS Region that you chose in step 4, the Region where you're creating the query logging configuration. If you choose to create a new resource, that resource will be created in the same Region.

VPCs to log queries for

This query logging configuration will log DNS queries that originate in the VPCs that you choose. Check the check box for each VPC in the current Region that you want Resolver to log queries for, then choose **Choose**.

Note

VPC log delivery can be enabled only once for a specific destination type. The logs can't be delivered to multiple destinations of the same type, for example, VPC logs can't be delivered to 2 Amazon S3 destinations.

7. Choose **Configure query logging**.

Note

You should start to see DNS queries made by resources in your VPC in the logs within a few minutes of successfully creating the query logging configuration.

Values that appear in Resolver query logs

Each log file contains one log entry for each DNS query that Amazon Route 53 received from DNS resolvers in the corresponding edge location. Each log entry includes the following values:

version

The version number of the query log format. The current version is 1.1.

The version value is a major and minor version in the form `major_version.minor_version`. For example, you can have a `version` value of 1.7, where 1 is the major version, and 7 is the minor version.

Route 53 increments the major version if a change is made to the log structure that is not backward-compatible. This includes removing a JSON field that already exists, or changing how the contents of a field are represented (for example, a date format).

Route 53 increments the minor version if a change adds new fields to the log file. This can occur if new information is available for some or all existing DNS queries within a VPC.

account_id

The ID of the AWS account that created the VPC.

region

The AWS Region that you created the VPC in.

vpc_id

The ID of the VPC that the query originated in.

query_timestamp

The date and time that the query was submitted, in ISO 8601 format and Coordinated Universal Time (UTC), for example, 2017-03-16T19:20:25.177Z.

For information about ISO 8601 format, see the Wikipedia article [ISO 8601](#). For information about UTC, see the Wikipedia article [Coordinated Universal Time](#).

query_name

The domain name (example.com) or subdomain name (www.example.com) that was specified in the query.

query_type

Either the DNS record type that was specified in the request, or ANY. For information about the types that Route 53 supports, see [Supported DNS record types \(p. 382\)](#).

query_class

The class of the query.

rcode

The DNS response code that Resolver returned in response to the DNS query. The response code indicates whether the query was valid or not. The most common response code is NOERROR, meaning that the query was valid. If the response is not valid, Resolver returns a response code that explains why not. For a list of possible response codes, see [DNS RCODEs](#) on the IANA website.

answer_type

The DNS record type (such as A, MX, or CNAME) of the value that Resolver is returning in response to the query. For information about the types that Route 53 supports, see [Supported DNS record types \(p. 382\)](#).

rdata

The value that Resolver returned in response to the query. For example, for an A record, this is an IP address in IPv4 format. For a CNAME record, this is the domain name in the CNAME record.

answer_class

The class of the Resolver response to the query.

srcaddr

The IP address of the instance that the query originated from.

srcport

The port on the instance that the query originated from.

transport

The protocol used to submit the DNS query.

srcids

IDs of the `instance`, `resolver_endpoint`, and the `resolver_network_interface` that the DNS query originated from or passed through.

instance

The ID of the instance that the query originated from.

resolver_endpoint

The ID of the resolver endpoint that passes the DNS query to on-premises DNS servers.

firewall_rule_group_id

The ID of the DNS Firewall rule group that matched the domain name in the query. This is populated only if DNS Firewall found a match for a rule with action set to alert or block.

For more information about the firewall rule groups, see [DNS Firewall rule groups and rules \(p. 560\)](#).

firewall_rule_action

The action specified by the rule that matched the domain name in the query. This is populated only if DNS Firewall found a match for a rule with action set to alert or block.

firewall_domain_list_id

The domain list used by the rule that matched the domain name in the query. This is populated only if DNS Firewall found a match for a rule with action set to alert or block.

Route 53 Resolver query log example

Here's a resolver query log example:

```
{  
    "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"  
}
```

Sharing Resolver query logging configurations with other AWS accounts

You can share the query logging configurations that you created using one AWS account with other AWS accounts. To share configurations, the Route 53 Resolver console integrates with AWS Resource Access Manager. For more information about Resource Access Manager, see the [Resource Access Manager User Guide](#).

Note the following:

Associating VPCs with shared query logging configurations

If another AWS account has shared one or more configurations with your account, you can associate VPCs with the configuration the same way that you associate VPCs with configurations that you created.

Deleting or unsharing a configuration

If you share a configuration with other accounts and then either delete the configuration or stop sharing it, and if one or more VPCs were associated with the configuration, Route 53 Resolver stops logging DNS queries that originate in those VPCs.

Maximum number of query logging configurations and VPCs that can be associated with a config

When an account creates a configuration and shares it with one or more other accounts, the maximum number of VPCs that can be associated with the configuration applies to the account that created the rule.

For current Resolver quotas, see [Quotas on Route 53 Resolver \(p. 673\)](#).

Permissions

To share a rule with another AWS account, you must have permission to use the [PutResolverQueryLogConfigPolicy](#) action.

Restrictions on the AWS account that a rule is shared with

The account that a rule is shared with can't change or delete the rule.

Tagging

Only the account that created a rule can add, delete, or see tags on the rule.

To view the current sharing status of a rule (including the account that shared the account or the account that a rule is shared with), and to share rules with another account, perform the following procedure.

To view sharing status and share query logging configurations with another AWS account

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Query Logging**.
3. On the navigation bar, choose the Region where you created the rule.

The **Sharing status** column shows the current sharing status of rules that were created by the current account or that are shared with the current account:

- **Not shared:** The current AWS account created the rule, and the rule is not shared with any other accounts.
 - **Shared by me:** The current account created the rule and shared it with one or more accounts.
 - **Shared with me:** Another account created the rule and shared it with the current account.
4. Choose the name of the rule that you want to display sharing information for or that you want to share with another account.

On the **Rule: rule name** page, the value under **Owner** displays ID of the account that created the rule. That's the current account unless the value of **Sharing status** is **Shared with me**. In that case, **Owner** is the account that created the rule and shared it with the current account.

5. Choose **Share** to view additional information or to share the rule with another account. A page in the Resource Access Manager console appears, depending on the value of **Sharing status**:
 - **Not shared:** The **Create resource share** page appears. For information about how to share the rule with another account, OU, or organization, skip to step 6.

- **Shared by me:** The **Shared resources** page shows the rules and other resources that are owned by the current account and shared with other accounts.
 - **Shared with me:** The **Shared resources** page shows the rules and other resources that are owned by other accounts and shared with the current account.
6. To share a query logging configuration with another AWS account, OU, or organization, specify the following values.

Note

You can't update sharing settings. If you want to change any of the following settings, you must reshare a rule with the new settings and then remove the old sharing settings.

Description

Enter a short description that helps you remember why you shared the query logging configuration.

Resources

Choose the check box for the configuration that you want to share.

Principals

Enter the AWS account number, OU name, or organization name.

Tags

Specify one or more keys and the corresponding values. For example, you might specify **Cost center** for **Key** and specify **456** for **Value**.

These are the tags that AWS Billing and Cost Management provides for organizing your AWS bill; you can use also tags for other purposes. For more information about using tags for cost allocation, see [Using cost allocation tags](#) in the *AWS Billing and Cost Management User Guide*.

Monitoring domain registrations

The Amazon Route 53 dashboard provides detailed information about the status of your domain registrations, including the following:

- Status of new domain registrations
- Status of domain transfers to Route 53
- List of domains that are approaching the expiration date

We recommend that you periodically check the dashboard in the Route 53 console, especially after you register a new domain or transfer a domain to Route 53, to confirm that there are no issues for you to address.

We also recommend that you confirm that the contact information for your domains is up to date. As the expiration date for a domain approaches, we email the registrant contact for the domain with information about when the domain expires and how to renew.

Monitoring your resources with Amazon Route 53 health checks and Amazon CloudWatch

You can monitor your resources by creating Amazon Route 53 health checks, which use CloudWatch to collect and process raw data into readable, near real-time metrics. These statistics are recorded for a

period of two weeks, so that you can access historical information and gain a better perspective on how your resources are performing. By default, metric data for Route 53 health checks is automatically sent to CloudWatch at one-minute intervals.

For more information about Route 53 health checks, see [Monitoring health checks using CloudWatch \(p. 532\)](#). For more information about CloudWatch, see [What is Amazon CloudWatch?](#) in the [Amazon CloudWatch User Guide](#).

Metrics and dimensions for Route 53 health checks

When you create a health check, Amazon Route 53 starts to send metrics and dimensions once a minute to CloudWatch about the resource that you specify. The Route 53 console lets you view the status of your health checks. You can also use the following procedures to view the metrics in the CloudWatch console or view them by using the AWS Command Line Interface (AWS CLI).

To view metrics using the CloudWatch console

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Metrics**.
3. On the **All Metrics** tab, choose **Route 53**.
4. Choose **Health Check Metrics**.

To view metrics using the AWS CLI

- At a command prompt, use the following command:

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Topics

- [CloudWatch metrics for Route 53 health checks \(p. 627\)](#)
- [Dimensions for Route 53 health check metrics \(p. 628\)](#)

CloudWatch metrics for Route 53 health checks

The AWS/Route53 namespace includes the following metrics for Route 53 health checks.

ChildHealthCheckHealthyCount

For a calculated health check, the number of health checks that are healthy among the health checks that Route 53 is monitoring.

Valid statistics: Average (recommended), Minimum, Maximum

Units: Healthy health checks

ConnectionTime

The average time, in milliseconds, that it took Route 53 health checkers to establish a TCP connection with the endpoint. You can view ConnectionTime for a health check either across all regions or for a selected geographic region.

Valid statistics: Average (recommended), Minimum, Maximum

Units: Milliseconds

HealthCheckPercentageHealthy

The percentage of Route 53 health checkers that consider the selected endpoint to be healthy. You can view `HealthCheckPercentageHealthy` only across all regions; data is not available for a selected region.

Valid statistics: Average, Minimum, Maximum

Units: Percent

HealthCheckStatus

The status of the health check endpoint that CloudWatch is checking. **1** indicates healthy, and **0** indicates unhealthy. You can view `HealthCheckStatus` only across all regions; data is not available for a selected region.

Valid statistics: Minimum

Units: none

SSLHandshakeTime

The average time, in milliseconds, that it took Route 53 health checkers to complete the SSL handshake. You can view `SSLHandshakeTime` for a health check either across all regions or for a selected geographic region.

Valid statistics: Average (recommended), Minimum, Maximum

Units: Milliseconds

TimeToFirstByte

The average time, in milliseconds, that it took Route 53 health checkers to receive the first byte of the response to an HTTP or HTTPS request. You can view `TimeToFirstByte` for a health check either across all regions or for a selected geographic region.

Valid statistics: Average (recommended), Minimum, Maximum

Units: Milliseconds

Dimensions for Route 53 health check metrics

Route 53 metrics for health checks use the AWS/Route53 namespace and provide metrics for `HealthCheckId`. When retrieving metrics, you must supply the `HealthCheckId` dimension.

In addition, for `ConnectionTime`, `SSLHandshakeTime`, and `TimeToFirstByte`, you can optionally specify `Region`. If you omit `Region`, CloudWatch returns metrics across all regions. If you include `Region`, CloudWatch returns metrics only for the specified region.

For more information, see [Monitoring health checks using CloudWatch \(p. 532\)](#).

Monitoring hosted zones using Amazon CloudWatch

You can monitor your public hosted zones by using Amazon CloudWatch to collect and process raw data into readable, near real-time metrics. Metrics are available shortly after Route 53 receives the DNS queries that the metrics are based on. CloudWatch metric data for Route 53 hosted zones has a granularity of one minute.

For more information, see the following documentation

- For an overview and information about how to view metrics in the Amazon CloudWatch console and how to retrieve metrics using the AWS Command Line Interface (AWS CLI), see [Viewing DNS query metrics for a public hosted zone \(p. 342\)](#)
- For information about the retention period for metrics, see [GetMetricStatistics](#) in the *Amazon CloudWatch API Reference*.
- For more information about CloudWatch, see [What is Amazon CloudWatch?](#) in the *Amazon CloudWatch User Guide*.
- For more information about CloudWatch metrics, see [Using Amazon CloudWatch metrics](#) in the *Amazon CloudWatch User Guide*.

Topics

- [CloudWatch metric for Route 53 public hosted zones \(p. 629\)](#)
- [CloudWatch dimension for Route 53 public hosted zone metrics \(p. 630\)](#)

CloudWatch metric for Route 53 public hosted zones

The AWS/Route53 namespace includes the following metric for Route 53 hosted zones:

DNSQueries

For all the records in a hosted zone, the number of DNS queries that Route 53 responds to in a specified time period.

Valid statistics: Sum, SampleCount

Units: Count

Region: Route 53 is a global service. To get hosted zone metrics, you must specify US East (N. Virginia) for the Region.

DNSSECInternalFailure

Value is 1 if any object in the hosted zone is in an INTERNAL_FAILURE state. Otherwise, value is 0.

Valid statistics: N/A

Units: Count

Volume: 1 per hosted zone per day

Region: Route 53 is a global service. To get hosted zone metrics, you must specify US East (N. Virginia) for the Region.

DNSSECKeySigningKeysNeedingAction

Number of key signing keys (KSKs) that have an ACTION_NEEDED state (due to KMS failure).

Valid statistics: Sum, SampleCount

Units: Count

Volume: 1 per hosted zone per day

Region: Route 53 is a global service. To get hosted zone metrics, you must specify US East (N. Virginia) for the Region.

DNSSECKeySigningKeyMaxNeedActionAge

Time elapsed since the key signing key (KSK) was set to the ACTION_NEEDED state.

Valid statistics: N/A

Units: Seconds

Volume: Up to 1 per hosted zone, per day

Region: Route 53 is a global service. To get hosted zone metrics, you must specify US East (N. Virginia) for the Region.

DNSSECKeySigningKeyAge

The time elapsed since the key signing key (KSK) was created (not since it was activated).

Valid statistics: N/A

Units: Seconds

Volume: 1 per hosted zone, per day

Region: Route 53 is a global service. To get hosted zone metrics, you must specify US East (N. Virginia) for the Region.

CloudWatch dimension for Route 53 public hosted zone metrics

Route 53 metrics for hosted zones use the AWS/Route53 namespace and provide metrics for HostedZoneId. To get the number of DNS queries, you must specify the ID of the hosted zone in the HostedZoneId dimension.

Monitoring Route 53 Resolver endpoints with Amazon CloudWatch

You can use Amazon CloudWatch to monitor the number of DNS queries that are forwarded by Route 53 Resolver endpoints. Amazon CloudWatch collects and processes raw data into readable, near real-time metrics. These statistics are recorded for a period of two weeks, so that you can access historical information and gain a better perspective on how your resources are performing. By default, metric data for Resolver endpoints is automatically sent to CloudWatch at five-minute intervals. The five-minute interval is also the smallest interval at which the metric data can be sent.

For more information about Resolver, see [Resolving DNS queries between VPCs and your network \(p. 471\)](#). For more information about CloudWatch, see [What is Amazon CloudWatch?](#) in the [Amazon CloudWatch User Guide](#).

Metrics and dimensions for Route 53 Resolver

When you configure Resolver to forward DNS queries to your network or vice versa, Resolver starts to send [metrics](#) and [dimensions](#) once every five minutes to CloudWatch about the number of queries that are forwarded. You can use the following procedures to view the metrics in the CloudWatch console or view them by using the AWS Command Line Interface (AWS CLI).

To view Resolver metrics using the CloudWatch console

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. On the navigation bar, choose the Region where you created the endpoint.
3. In the navigation pane, choose **Metrics**.
4. On the **All metrics** tab, choose **Route 53 Resolver**.
5. Choose **By Endpoint** to view query counts for a specified endpoint. Then choose the endpoints that you want to view the number of queries for.

Choose **Across All Endpoints** to view query counts for all inbound endpoints or for all outbound endpoints that were created by the current AWS account. Then choose **InboundQueryVolume** or **OutboundQueryVolume** to view the desired counts.

To view metrics using the AWS CLI

- At a command prompt, use the following command:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Topics

- [CloudWatch metrics for Route 53 Resolver \(p. 631\)](#)
- [Dimensions for Route 53 Resolver metrics \(p. 633\)](#)

CloudWatch metrics for Route 53 Resolver

The `AWS/Route53Resolver` namespace includes metrics for Route 53 Resolver endpoints and for IP addresses.

Topics

- [Metrics for Resolver endpoints \(p. 631\)](#)
- [Metrics for Resolver IP addresses \(p. 632\)](#)

Metrics for Resolver endpoints

The `AWS/Route53Resolver` namespace includes the following metrics for Route 53 Resolver endpoints.

EndpointHealthyENICount

The number of elastic network interfaces in the `OPERATIONAL` status. This means that the Amazon VPC network interfaces for the endpoint (specified by `EndpointId`) are correctly configured and able to pass inbound or outbound DNS queries between your network and Resolver.

Valid statistics: Minimum, Maximum, Average

Units: Count

EndpointUnHealthyENICount

The number of elastic network interfaces in the `AUTO_RECOVERING` status.

This means that the resolver is trying to recover one or more of the Amazon VPC network interfaces that are associated with the endpoint (specified by `EndpointId`). During the recovery process,

the endpoint functions with limited capacity and is unable to process DNS queries until it's fully recovered.

Valid statistics: Minimum, Maximum, Average

Units: Count

InboundQueryVolume

For inbound endpoints, the number of DNS queries forwarded from your network to your VPCs through the endpoint specified by `EndpointId`.

Valid statistics: Sum

Units: Count

OutboundQueryVolume

For outbound endpoints, the number of DNS queries forwarded from your VPCs to your network through the endpoint specified by `EndpointId`.

Valid statistics: Sum

Units: Count

OutboundQueryAggregateVolume

For outbound endpoints, the total number of DNS queries forwarded from Amazon VPCs to your network, including the following:

- The number of DNS queries forwarded from your VPCs to your network through the endpoint that is specified by `EndpointId`.
- When the current account shares Resolver rules with other accounts, queries from VPCs that are created by other accounts that are forwarded to your network through the endpoint that is specified by `EndpointId`.

Valid statistics: Sum

Units: Count

Metrics for Resolver IP addresses

The `AWS/Route53Resolver` namespace includes the following metrics for each IP address that's associated with a Resolver inbound or outbound endpoint. (When you specify an endpoint, Resolver creates an Amazon VPC [elastic network interface](#).)

InboundQueryVolume

For each IP address for your inbound endpoints, the number of DNS queries forwarded from your network to the specified IP address. Each IP address is identified by the IP address ID. You can get this value using the Route 53 console. On the page for the applicable endpoint, in the IP addresses section, see the **IP address ID** column. You can also get the value programmatically using [ListResolverEndpointIpAddresses](#).

Valid statistics: Sum

Units: Count

OutboundQueryAggregateVolume

For each IP address for your outbound endpoints, the total number of DNS queries forwarded from Amazon VPCs to your network, including the following:

- The number of DNS queries forwarded from your VPCs to your network using the specified IP address.
- When the current account shares Resolver rules with other accounts, queries from VPCs that are created by other accounts that are forwarded to your network through using the specified IP address.

Each IP address is identified by the IP address ID. You can get this value using the Route 53 console. On the page for the applicable endpoint, in the IP addresses section, see the **IP address ID** column. You can also get the value programmatically using [ListResolverEndpointIpAddresses](#).

Valid statistics: Sum

Units: Count

Dimensions for Route 53 Resolver metrics

Route 53 Resolver metrics for inbound and outbound endpoints use the `AWS/Route53Resolver` namespace and provide metrics for `EndpointId`. If you specify a value for the `EndpointId` dimension, CloudWatch returns the number of DNS queries for the specified endpoint. If you don't specify `EndpointId`, CloudWatch returns the number of DNS queries for all endpoints that were created by the current AWS account.

Monitoring Route 53 Resolver DNS Firewall rule groups with Amazon CloudWatch

You can use Amazon CloudWatch to monitor the number of DNS queries that are filtered by Route 53 Resolver DNS Firewall rule groups. Amazon CloudWatch collects and processes raw data into readable, near real-time metrics. These statistics are recorded for a period of two weeks, so that you can access historical information and gain a better perspective on how your resources are performing. By default, metric data for DNS Firewall rule groups is automatically sent to CloudWatch at five-minute intervals.

For more information about DNS Firewall, see [Route 53 Resolver DNS Firewall \(p. 554\)](#). For more information about CloudWatch, see [What is Amazon CloudWatch?](#) in the *Amazon CloudWatch User Guide*.

Metrics and dimensions for Route 53 Resolver DNS Firewall

When you associate a Route 53 Resolver DNS Firewall rule group with a VPC to filter DNS queries, DNS Firewall starts to send metrics and dimensions once every 5 minutes to CloudWatch about the queries that it filters. For information about the metrics and dimensions for DNS Firewall, see [CloudWatch metrics for Route 53 Resolver DNS Firewall \(p. 634\)](#).

You can use the following procedures to view the metrics in the CloudWatch console or view them by using the AWS Command Line Interface (AWS CLI).

To view DNS Firewall metrics using the CloudWatch console

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. On the navigation bar, choose the Region that you want to view.
3. In the navigation pane, choose **Metrics**.
4. On the **All metrics** tab, choose **Route 53 Resolver**.
5. Choose a metric that you're interested in.

To view metrics using the AWS CLI

- At a command prompt, use the following command:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Topics

- [CloudWatch metrics for Route 53 Resolver DNS Firewall \(p. 634\)](#)

CloudWatch metrics for Route 53 Resolver DNS Firewall

The `AWS/Route53Resolver` namespace includes metrics for Route 53 Resolver DNS Firewall rule groups.

Topics

- [Metrics for Route 53 Resolver DNS Firewall rule groups \(p. 634\)](#)
- [Metrics for VPCs \(p. 634\)](#)
- [Metrics for firewall rule group and VPC association \(p. 634\)](#)
- [Metrics for a domain list in a firewall rule group \(p. 635\)](#)

Metrics for Route 53 Resolver DNS Firewall rule groups

FirewallRuleGroupQueryVolume

The number of DNS Firewall queries that match a firewall rule group (specified by `FirewallRuleGroupId`).

Dimensions: `FirewallRuleGroupId`

Valid statistics: Sum

Units: Count

Metrics for VPCs

VPCFirewallQueryVolume

The number of DNS Firewall queries from a VPC (specified by `VpcId`).

Dimensions: `VpcId`

Valid statistics: Sum

Units: Count

Metrics for firewall rule group and VPC association

FirewallRuleGroupVpcQueryVolume

The number of DNS Firewall queries from a VPC (specified by `VpcId`) that match a firewall rule group (specified by `FirewallRuleGroupId`).

Dimensions: `FirewallRuleGroupId`, `VpcId`

Valid statistics: Sum

Units: Count

Metrics for a domain list in a firewall rule group

FirewallRuleGroupVpcQueryVolume

The number of DNS firewall queries that match a firewall domain list (specified by `FirewallDomainListId`) within a firewall rule group (specified by `FirewallRuleGroupId`).

Dimensions: `FirewallRuleGroupId`, `FirewallDomainListId`

Valid statistics: Sum

Units: Count

Logging Amazon Route 53 API calls with AWS CloudTrail

Route 53 is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Route 53. CloudTrail captures all API calls for Route 53 as events, including calls from the Route 53 console and from code calls to the Route 53 APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Route 53. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Route 53, the IP address that the request was made from, who made the request, when it was made, and additional details.

Topics

- [Route 53 information in CloudTrail \(p. 635\)](#)
- [Viewing Route 53 events in event history \(p. 636\)](#)
- [Understanding Route 53 log file entries \(p. 636\)](#)

Route 53 information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Route 53, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing events with CloudTrail event history](#).

For an ongoing record of events in your AWS account, including events for Route 53, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all regions. The trail logs events from all regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- [Overview for creating a trail](#)
- [CloudTrail supported services and integrations](#)
- [Configuring Amazon SNS notifications for CloudTrail](#)

- Receiving CloudTrail log files from multiple Regions and Receiving CloudTrail log files from multiple accounts

All Route 53 actions are logged by CloudTrail and are documented in the [Amazon Route 53 API Reference](#). For example, calls to the `CreateHostedZone`, `CreateHealthCheck`, and `RegisterDomain` actions generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail userIdentity element](#).

Viewing Route 53 events in event history

CloudTrail lets you view recent events in **Event history**. To view events for Route 53 API requests, you must choose **US East (N. Virginia)** in the region selector at the top of the console. For more information, see [Viewing events with CloudTrail event history](#) in the *AWS CloudTrail User Guide*.

Understanding Route 53 log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The `eventName` element identifies the action that occurred. (In CloudTrail logs, the first letter is lowercase for domain registration actions even though it's uppercase in the names of the actions. For example, `UpdateDomainContact` appears as `updateDomainContact` in the logs). CloudTrail supports all Route 53 API actions. The following example shows a CloudTrail log entry that demonstrates the following actions:

- List the hosted zones that are associated with an AWS account
- Create a health check
- Create two records
- Delete a hosted zone
- Update information for a registered domain
- Create a Route 53 Resolver outbound endpoint

```
{  
    "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",  
            "identity": {  
                "accessKeyId": "AKIAJLW46PQH4V5K5OQ",  
                "accountId": "123456789012",  
                "callerArn": "arn:aws:sts::123456789012:assumed-role/Route53ServiceRole/CloudTrail",  
                "principal": "CloudTrail",  
                "region": "us-east-1",  
                "type": "AWS",  
                "user": "CloudTrail"}
```

```

    "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": "44445556666",
"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-ebee-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": "4444455556666"
},
{
    "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"
}
]
```

Troubleshooting Amazon Route 53

The topics in this chapter can help you troubleshoot problems with your domain registration and DNS configuration.

Topics

- [My domain is unavailable on the internet \(p. 642\)](#)
- [My domain is suspended \(status is ClientHold\) \(p. 646\)](#)
- [Transferring my domain to Amazon Route 53 failed \(p. 648\)](#)
- [I changed DNS settings, but they haven't taken effect \(p. 649\)](#)
- [My browser displays a "Server not found" error \(p. 652\)](#)
- [I can't route traffic to an Amazon S3 bucket that's configured for website hosting \(p. 652\)](#)
- [I was billed twice for the same hosted zone \(p. 653\)](#)
- [My AWS account is closed, suspended, or terminated, and my domain is registered with Route 53 \(p. 653\)](#)

My domain is unavailable on the internet

Here are the most common reasons that your domain is not available on the internet.

Topics

- [You registered a new domain, but you didn't click the link in the confirmation email \(p. 642\)](#)
- [You transferred domain registration to Amazon Route 53, but you didn't transfer DNS service \(p. 643\)](#)
- [You transferred domain registration and specified the wrong name servers in the domain settings \(p. 643\)](#)
- [You transferred DNS service first, but you didn't wait long enough before transferring domain registration \(p. 644\)](#)
- [You deleted the hosted zone that Route 53 is using to route internet traffic for the domain \(p. 645\)](#)
- [Your domain has been suspended \(p. 645\)](#)

You registered a new domain, but you didn't click the link in the confirmation email

When you register a new domain, ICANN requires that we get confirmation that the email address for the registrant contact is valid. To get confirmation, we send an email that contains a link. (If you don't respond to the first email, we resend the same email up to two more times.) You have between 3 and 15 days to click the link, depending on the top-level domain. After that time, the link stops working.

If you don't click the link in the email in the allotted amount of time, ICANN requires that we suspend the domain. For information about how to resend the confirmation email to the registrant contact, see [Resending authorization and confirmation emails \(p. 86\)](#).

You transferred domain registration to Amazon Route 53, but you didn't transfer DNS service

If your previous registrar offered free DNS service with domain registration, the registrar might have stopped providing DNS service when you transferred domain registration to Route 53. Perform the following procedure to determine whether this is the problem and, if so, to resolve it.

To restore DNS service if your previous registrar canceled it after you transferred domain registration to Route 53

1. Contact your previous registrar and confirm that they canceled DNS service for your domain. If so, here are the three quickest ways to restore DNS service for the domain, in order of desirability:
 - If the previous registrar provides paid DNS service, ask them to restore DNS service using the old DNS records and name servers for your domain.
 - If the previous registrar doesn't provide paid DNS service without domain registration, ask whether you can transfer domain registration back to them and have them restore DNS service using the old DNS records and name servers for your domain.
 - If you can transfer domain registration back to the previous registrar but they don't have your DNS records any longer, ask whether you can transfer domain registration back to them and get the same set of name servers that were formerly assigned to the domain. If this is possible, you'll have to recreate your old DNS records yourself. However, as soon as you do that, your domain will become available again.

If your previous registrar can't help with any of these options, continue with step 2.

Important

If you can't restore DNS service using the name servers that you specified when you transferred your domain to Route 53, it can take up to two days after you complete the remaining steps in this procedure for your domain to become available again on the internet. DNS resolvers typically cache the names of the name servers for a domain for 24 to 48 hours, and it will take that long before all DNS resolvers get the names of the new name servers.

2. Choose a new DNS service, for example, Route 53.
3. Using the method provided by the new DNS service, create a hosted zone and records:
 - a. Create a hosted zone that has the same name as your domain, such as example.com.
 - b. Use the zone file that you got from the previous registrar to create records.

If you chose Route 53 as your new DNS service, you can create records by importing the zone file. For more information, see [Creating records by importing a zone file \(p. 438\)](#).

4. Get the name servers for the new hosted zone. If you chose Route 53 as the DNS service, see [Getting the name servers for a public hosted zone \(p. 341\)](#).
5. Change the name servers for your domain to the name servers that you got in step 4. For more information, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#).

You transferred domain registration and specified the wrong name servers in the domain settings

When you transfer domain registration to Amazon Route 53, one of the settings that you specify for the domain is the set of name servers that will respond to DNS queries for the domain. These name

servers come from the hosted zone that has the same name as the domain. The hosted zone contains information about how you want to route traffic for the domain, such as the IP address of a web server for `www.example.com`.

You might have accidentally specified the name servers for the wrong hosted zone, which is especially easy if you have more than one hosted zone that has the same name as the domain. To confirm that the domain is using the name servers for the correct hosted zone and, if necessary, update the name servers for the domain, perform the following procedures.

Important

If you specified the wrong name server records when you transferred the domain to Route 53, it can take up to two days after you correct the name servers for the domain before DNS service is fully restored. This is because DNS resolvers across the internet typically request the name servers only once every two days and cache the answer.

To get the name servers for your hosted zone

1. If you're using another DNS service for the domain, use the method provided by the DNS service to get the name servers for the hosted zone. Then skip to the next procedure.
If you're using Route 53 as the DNS service for the domain, sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53>.
2. In the navigation pane, choose **Hosted Zones**.
3. On the **Hosted Zones** page, choose the radio button (not the name) for the hosted zone.
Important
If you have more than one hosted zone with the same name, make sure you're getting the name servers for the correct hosted zone.
4. In the right pane, make note of the four servers listed for **Name Servers**.

To confirm that the domain is using the correct name servers

1. If you're using another DNS service for the domain, sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53>
If you're using Route 53, skip to the next step.
2. In the navigation pane, choose **Registered Domains**.
3. Choose the name of the domain for which you want to edit settings.
4. Choose **Add or Edit Name Servers**.
5. Compare the list of name servers that you got in the previous procedure with the name servers that are listed in the **Edit Name Servers for domain name** dialog box.
6. If the name servers listed here don't match the name servers that you got in the previous procedure, change the name servers here, and then choose **Update**.

You transferred DNS service first, but you didn't wait long enough before transferring domain registration

When you transferred DNS service to Amazon Route 53 or another DNS service, you updated the configuration for your domain with the domain registrar to use the name servers for the new DNS service.

DNS resolvers, which respond to requests for your domain, commonly cache the names of name servers for 24 to 48 hours. If you change the DNS service for a domain and replace the name servers from one DNS service with the name servers for another DNS service, it can take up to 48 hours before DNS resolvers start using the new name servers and, therefore, the new DNS service.

Here's how transferring your DNS service and then transferring your domain too soon after can cause your domain to become unavailable on the internet:

1. You transferred DNS service for your domain.
2. You transferred your domain to Route 53 before DNS resolvers started to use the name servers for your new DNS service.
3. Your previous registrar canceled DNS service for your domain as soon as the domain was transferred to Route 53.
4. DNS resolvers are still routing queries to your old DNS service, but there are no longer any records that tell how to route your traffic.

When caching expires for the name servers for the old DNS service, DNS will start to use your new DNS service. Unfortunately, there is no way to accelerate this process.

You deleted the hosted zone that Route 53 is using to route internet traffic for the domain

If Route 53 is the DNS service for your domain and if you delete the hosted zone that is used to route internet traffic for the domain, the domain will become unavailable on the internet. This is true regardless of whether the domain is registered with Route 53.

Important

Restoring internet service for the domain can take up to 48 hours.

To restore internet service if you delete a hosted zone that Route 53 is using to route internet traffic for a domain

1. Create another hosted zone that has the same name as the domain. For more information, see [Creating a public hosted zone \(p. 340\)](#).
2. Recreate the records that were in the hosted zone that you deleted. For more information, see [Working with records \(p. 370\)](#).
3. Get the names of the name servers that Route 53 assigned to the new hosted zone. For more information, see [Getting the name servers for a public hosted zone \(p. 341\)](#).
4. Update the domain registration to use the name servers that you got in step 3:
 - If the domain is registered with Route 53, see [Adding or changing name servers and glue records for a domain \(p. 61\)](#).
 - If the domain is registered with another domain registrar, use the method provided by the registrar to update the domain registration to use the new name servers.
5. Wait for the TTL for the name servers to pass for recursive resolvers that have cached the names of the name servers for the deleted hosted zone. After the TTL has passed, when a browser or application submits a DNS query for the domain or one of its subdomains, a recursive resolver forwards the query to the Route 53 name servers for the new hosted zone. For more information, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

The TTL for name servers can be as long as 48 hours, depending on the TLD of the domain.

Your domain has been suspended

Your domain might be unavailable on the internet because we had to suspend it. For more information, see [My domain is suspended \(status is ClientHold\) \(p. 646\)](#).

My domain is suspended (status is ClientHold)

If Amazon Route 53 suspends your domain, the domain becomes unavailable on the internet. You can use either of the following methods to determine whether a domain has been suspended:

- On the **Registered domains** page of the Route 53 console, find the domain name in the **Alerts** table at the bottom of the page. If the value of the **Status** column is **clientHold**, the domain has been suspended.
- Send a WHOIS query for the domain. If the value of **Domain Status** is **clientHold**, the domain has been suspended. The WHOIS command is available in many operating systems, and it's also available as a web application on many websites.

In addition, when we suspend a domain, we generally send an email to the email address for the registrant contact for the domain. However, if the domain was suspended based on a court order, the court might not let us notify the registrant contact.

To make a domain available on the internet again, you must get it unsuspended. Here are the reasons that a domain can be suspended and how you get it unsuspended.

Note

If you need help getting your domain unsuspended, you can contact AWS Support free of charge. For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

Topics

- [You registered a new domain, but you didn't click the link in the confirmation email \(p. 646\)](#)
- [You disabled automatic renewal for the domain, and the domain expired \(p. 647\)](#)
- [You changed the email address for the registrant contact, but you didn't verify that the new email address is valid \(p. 647\)](#)
- [We couldn't process your payment for automatic domain renewal, and the domain expired \(p. 647\)](#)
- [We suspended the domain for a violation of the AWS Acceptable Use Policy \(p. 647\)](#)
- [We suspended the domain because of a court order \(p. 648\)](#)

You registered a new domain, but you didn't click the link in the confirmation email

When you register a domain with AWS for the first time, ICANN requires that we get confirmation that the email address for the registrant contact is valid. To get confirmation, we send an email that contains a link. You have between 3 and 15 days to click the link, depending on the top-level domain. After that time, the link stops working.

Note

If you don't respond to the first email, we resend the email up to two more times. If you have already registered one or more domains with Amazon Route 53 and used the same email address for the registrant contact, we don't send a confirmation email.

If you don't click the link in the email in the allotted amount of time, ICANN requires that we suspend the domain. For information about how to resend the confirmation email to the registrant contact, see [Resending authorization and confirmation emails \(p. 86\)](#). When you confirm that the email address is valid, we automatically unsuspend the domain.

You disabled automatic renewal for the domain, and the domain expired

When automatic renewal is enabled for a domain (the default value for a new or transferred domain), we automatically renew registration for the domain shortly before the expiration date. If you disable automatic renewal, we send three reminder emails that the domain registration is about to expire to the email address for the registrant contact. We start to send these emails 45 days before the domain expires.

If you disable automatic renewal for the domain and you don't manually extend the registration period for the domain, we generally suspend the domain on the expiration date. Note that the registries for some domains delete the domain even before the expiration date.

For information about how to renew an expired domain, see [Renewing registration for a domain \(p. 63\)](#).

You changed the email address for the registrant contact, but you didn't verify that the new email address is valid

If you change the email address for the registrant contact to an address that you haven't previously verified, ICANN requires that we get confirmation that the email address for the registrant contact is valid. To get confirmation, we send an email that contains a link. You have between 3 and 15 days to click the link, depending on the top-level domain. After that time, the link stops working.

If you don't click the link in the email in the amount of time allowed by the TLD registry, ICANN requires that we suspend the domain. For information about how to resend the confirmation email to the registrant contact, see [Resending authorization and confirmation emails \(p. 86\)](#). When you confirm that the email address is valid, we automatically unsuspend the domain.

We couldn't process your payment for automatic domain renewal, and the domain expired

If automatic renewal is enabled for a domain but we weren't able to process your payment (for example, because your credit card expired), we send several emails to the email address for the registrant contact for the domain. If we don't receive payment, we generally suspend the domain on the expiration date. Note that the registries for some domains delete the domain even before the expiration date.

For information about how to renew an expired domain, see [Renewing registration for a domain \(p. 63\)](#).

We suspended the domain for a violation of the AWS Acceptable Use Policy

If we suspend a domain for a violation of the [AWS Acceptable Use Policy](#), we send an email notification to the registrant contact for the domain. (We don't send a notification email if the AWS account is already suspended for fraud.)

To contest a suspension, send an email to abuse@amazon.com.

We suspended the domain because of a court order

If a domain is suspended as a result of a court order, we can't unsuspend the domain until the court order has been lifted. To contest the validity of a court order, send an email to abuse@amazon.com and attach the applicable documents.

Transferring my domain to Amazon Route 53 failed

Here are some common reasons that transferring a domain to Amazon Route 53 fails.

Topics

- [You didn't click the link in the authorization email \(p. 648\)](#)
- [The authorization code that you got from the current registrar is not valid \(p. 648\)](#)
- ["Parameters in request are not valid" error when trying to transfer a .es domain to Amazon Route 53 \(p. 649\)](#)

You didn't click the link in the authorization email

When you transfer domain registration to Amazon Route 53, we're required by ICANN, the governing body for domain registration, to get authorization for the transfer from the registrant contact for the domain. To get authorization, we send you an email that contains a link. You have between 5 and 15 days to click the link, depending on the top-level domain. After that time, the link stops working.

If you don't click the link in the email in the allotted amount of time, ICANN requires that we cancel the transfer. For information about how to resend the authorization email to the registrant contact, see [Resending authorization and confirmation emails \(p. 86\)](#).

The authorization code that you got from the current registrar is not valid

If you request the transfer of a domain to Amazon Route 53 and you don't receive the authorization email, check [the status page in the Route 53 console](#). If the status page shows that the transfer authorization code that you got from your registrar is not valid, perform the following steps:

1. Contact the current registrar for the domain and request a new authorization code. Confirm the following:
 - How long the new authorization code will remain active. You must request a domain transfer before the code expires.
 - The new authorization code is different from the code that isn't valid. If not, ask the current registrar to refresh the authorization code.
2. Submit another request to transfer the domain. For more information, see [Step 5: Request the transfer \(p. 71\)](#) in the topic [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#).

"Parameters in request are not valid" error when trying to transfer a .es domain to Amazon Route 53

Amazon Route 53 returns a "Parameters in request are not valid" error when you try to transfer a .es domain to Route 53 and the contact type of the registrant contact is **Company**. To complete the transfer, change the contact type of the registrant to **Person**, and re-submit.

I changed DNS settings, but they haven't taken effect

If you changed DNS settings, here are some common reasons that the changes haven't taken effect yet.

Topics

- You transferred DNS service to Amazon Route 53 in the last 48 hours, so DNS is still using your previous DNS service (p. 649)
- You recently transferred DNS service to Amazon Route 53, but you didn't update the name servers with the domain registrar (p. 649)
- DNS resolvers still are using the old settings for the record (p. 650)
- You have more than one hosted zone with the same name, and you updated the one that isn't associated with the domain (p. 651)

You transferred DNS service to Amazon Route 53 in the last 48 hours, so DNS is still using your previous DNS service

When you transferred DNS service to Amazon Route 53, you used the method provided by the registrar for your domain to replace the name servers for the previous DNS service with the four name servers for Route 53.

Note

If you aren't sure you did this part, see [You recently transferred DNS service to Amazon Route 53, but you didn't update the name servers with the domain registrar \(p. 649\)](#).

Domain registrars typically use a TTL (time to live) of 24 to 48 hours for name servers. This means that when a DNS resolver gets the name servers for your domain, it uses that information for up to 48 hours before it submits another request for the current name servers for the domain. If you transferred DNS service to Route 53 in the last 48 hours and then changed DNS settings, some DNS resolvers are still using your old DNS service to route traffic for the domain.

You recently transferred DNS service to Amazon Route 53, but you didn't update the name servers with the domain registrar

The registrar for your domain has a variety of information about the domain, including the name servers for the DNS service for the domain. Typically, the domain registrar is also your DNS service, so the name servers that are associated with your domain belong to the registrar. These name servers tell DNS where

to get information about how you want traffic for your domain to be routed, for example, to the IP address of a web server for your domain.

When you transfer DNS service to Amazon Route 53, you need to use the method that is provided by your domain registrar to change the name servers that are associated with your domain. You're usually replacing the name servers that are provided by the registrar with the four Route 53 name servers that are associated with the hosted zone that you created for the domain.

If you created a new hosted zone and records for your domain and specified different settings than you used for the previous DNS service, and if DNS is still routing traffic to the old resources, it's possible that you didn't update the name servers with the domain registrar. To determine whether the registrar is using the name servers for your Route 53 hosted zone and, if necessary, to update the name servers for the domain, perform the following procedure:

To get the name servers for your hosted zone and update the name server setting with the domain registrar

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. In the navigation pane, choose **Hosted Zones**.
3. On the **Hosted Zones** page, choose the name of the hosted zone (not the radio button) for the hosted zone.

Important

If you have more than one hosted zone with the same name, make sure you're getting the name servers for the correct hosted zone.

4. In the **Record name** list, make note of the four servers listed for **Name Servers**.
5. Using the method provided by the registrar for the domain, display the list of name servers for the domain.
6. If the name servers for the domain match the name servers that you got in step 4, then the domain configuration is correct.

If the name servers for the domain don't match the name servers that you got in step 4, update the domain to use the Route 53 name servers.

- 7.

Important

When you change the name servers for the domain to the name servers from your Route 53 hosted zone, it can take up to two days for the change to take effect and for Route 53 to become your DNS service. This is because DNS resolvers across the internet typically request the name servers only once every two days and cache the answer.

DNS resolvers still are using the old settings for the record

If you changed the settings in a record but your traffic is still being routed to the old resource, such as a web server for your website, one possible cause is that DNS still has the previous settings cached. Each record has a TTL (time to live) value that specifies how long, in seconds, that you want DNS resolvers to cache the information in the record, such as the IP address for a web server. Until the amount of time that is specified by the TTL passes, DNS resolvers will continue to return the old value in response to DNS queries. If you want to know what the TTL is for a record, perform the following procedure.

Note

For alias records, the TTL is determined by the AWS resource that the record routes traffic to. For more information, see [Choosing between alias and non-alias records \(p. 379\)](#).

To view the TTL for a record

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. On the **Hosted Zones** page, choose the name of the hosted zone that includes the record.
3. In the list of records, find the record that you want the TTL value for, and check the value of the **TTL** column.

Note

Changing the TTL now won't make your change take effect faster. DNS resolvers already have the value cached, and they won't get the new setting until the amount of time that was specified by the old setting passes.

You have more than one hosted zone with the same name, and you updated the one that isn't associated with the domain

You can create more than one hosted zone that has the same name, either using the same account or using multiple accounts. To specify the hosted zone that Route 53 uses to route internet traffic for your domain, you get the four Route 53 name servers for that hosted zone, and you update the domain registration to use those name servers.

If you add, change, or delete records in one hosted zone but your domain registration is using the name servers for another hosted zone, Route 53 responses to DNS queries won't reflect your changes. To determine whether your domain registration is using the name servers for the hosted zone that you updated records in, perform the following tasks:

1. Determine which name servers are associated with your domain registration. See [Adding or changing name servers or glue records \(p. 62\)](#).
2. Compare the name servers that you got in step 1 with the name servers that Route 53 assigned to the hosted zone that you updated records in. See [Getting the name servers for a public hosted zone \(p. 341\)](#).

If the name servers for the domain registration don't match the name servers for the hosted zone that you updated records in, you have two options:

Change records in the hosted zone that's currently associated with the domain (recommended)

Make note of the changes that you made in the hosted zone that is not currently associated with your domain registration. Then go to the hosted zone that is associated with the domain registration, and make the same changes. This is the preferred method because the changes take effect almost immediately. For more information, see [Editing records \(p. 440\)](#).

Update your domain registration to use different name servers

Change your domain registration to use the name servers in the hosted zone that you updated.

Important

If you change the name servers that are associated with your domain registration, your domain will be unavailable on the internet for up to 2 days. This is because DNS resolvers typically cache the names of name servers for 2 days. For an overview of how DNS works, including information about resolver caching, see [How Amazon Route 53 routes traffic for your domain \(p. 3\)](#).

By changing the name servers that are associated with your domain registration, you're essentially changing the DNS service for the domain. You have two options, depending on whether the domain is currently in use:

- If the domain is in use, see [Making Route 53 the DNS service for a domain that's in use \(p. 326\)](#).
- If the domain is currently inactive, perform the following tasks:
 1. Get the name servers for the hosted zone that you want to use to route traffic to your domain. See [Getting the name servers for a public hosted zone \(p. 341\)](#).
 2. In the hosted zone that you got name servers for in step 1, confirm that the NS record is using the same four name servers. If not, update the NS record. See [Editing records \(p. 440\)](#).
 3. Update the domain registration to use the name servers that you got in step 1. See [Adding or changing name servers or glue records \(p. 62\)](#).

My browser displays a "Server not found" error

If your browser displays a "Server not found" error when you try to browse to a domain (example.com) or a subdomain (www.example.com), here are some common explanations.

Topics

- [You didn't create a record for the domain or subdomain name \(p. 652\)](#)
- [You created a record but specified the wrong value \(p. 652\)](#)
- [The resource that you're routing traffic to is unavailable \(p. 652\)](#)

You didn't create a record for the domain or subdomain name

If you don't create a record for the domain or subdomain, then DNS doesn't know where to route traffic when someone enters that name in a browser. For more information, see [Working with records \(p. 370\)](#).

You created a record but specified the wrong value

When you create a record, it's easy to specify the wrong value, such as the IP address for a web server or the domain name that CloudFront assigned to your web distribution. If the record exists but you're still getting a "Server not found" error, we recommend that you confirm that the value is correct.

The resource that you're routing traffic to is unavailable

If a record specifies a resource such as a web server that's unavailable, a browser will return a "Server not found" error. We recommend that you check the status of the resource that you're routing traffic to.

I can't route traffic to an Amazon S3 bucket that's configured for website hosting

When you configure an Amazon S3 bucket for website hosting, you must give the bucket the same name as the record that you want to use to route traffic to the bucket. For example, if you want to route traffic

for example.com to an S3 bucket that is configured for website hosting, the name of the bucket must be example.com.

If you want to route traffic to an S3 bucket that is configured for website hosting but the name of the bucket doesn't appear in the **Alias Target** list in the Amazon Route 53 console, or if you're trying to create an alias record programmatically and you're getting an `InvalidInput` error from the Route 53 API, one of the AWS SDKs, the AWS CLI, or AWS Tools for Windows PowerShell, check the following:

- The name of the bucket exactly matches the name of the record, such as example.com or www.example.com.
- The S3 bucket is correctly configured for website hosting. For more information, see [Hosting a static website on Amazon S3](#) in the *Amazon Simple Storage Service User Guide*.

I was billed twice for the same hosted zone

We don't bill you if you delete a hosted zone within 12 hours after you create it. After 12 hours, we immediately charge the standard monthly fee for a hosted zone. The monthly charge for a hosted zone is not prorated for partial months. (The same charge applies for the hosted zone that we automatically create when you register a domain.)

If you create a hosted zone on the last day of the month (for example, January 31), the charge for January might appear on the February invoice, along with the charge for February. Note that Amazon Route 53 uses Coordinated Universal Time (UTC) as the time zone to determine when a hosted zone was created.

My AWS account is closed, suspended, or terminated, and my domain is registered with Route 53

If you closed your AWS account, or if the account is suspended or terminated, Route 53 doesn't automatically renew your domain registration even if automatic renewal is turned on. You can contact AWS Support and ask them for help with the following options:

- If you don't want to keep the domain registration, AWS Support can disable automatic renewal for the domain. This prevents you from getting several reminder emails about domain renewal.
- If you do want to keep the domain registration, AWS Support can help you transfer the domain registration to another AWS account.
- AWS Support can also help you transfer the domain to another domain registrar.

For more information, see [Contacting AWS Support about domain registration issues \(p. 95\)](#).

IP address ranges of Amazon Route 53 servers

Amazon Web Services (AWS) publishes its current IP address ranges in JSON format. If your firewalls or security groups restrict incoming traffic based on source IP addresses, confirm that your configuration allows traffic from the applicable IP address ranges.

To view the current IP address ranges for Route 53, download [ip-ranges.json](#), and search the file for the following values:

"service": "ROUTE53"

These IP address ranges are used by Route 53 name servers. Add these ranges to the list of allowed IP address ranges if you're using Route 53 as the DNS service for one or more domains and you want to be able to use the `dig` or `nslookup` commands to query Route 53 name servers.

Note

We rarely change the IP addresses of name servers; if we need to change IP addresses, we'll notify you in advance.

"service": "ROUTE53_HEALTHCHECKS"

These IP address ranges are used by Route 53 health checkers. Add these ranges to the list of allowed IP address ranges if you're using Route 53 health checks to check the health of resources on your network.

Note

We rarely change the IP addresses of health checkers; if we need to change IP addresses, we'll notify you in advance.

For more information about IP addresses for health checks, see [Configuring router and firewall rules for Amazon Route 53 health checks \(p. 529\)](#).

"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"

Route 53 uses these IP address ranges only internally. You don't need to add these ranges to the list of allowed ranges.

For more information about IP addresses for AWS resources, see [AWS IP address ranges](#) in the *Amazon Web Services General Reference*.

Tagging Amazon Route 53 resources

A tag is a label that you assign to an AWS resource. Each tag consists of a *key* and a *value*, both of which you define. For example, the key might be "domain" and the value might be "example.com". You can use tags for a variety of purposes; one common use is to categorize and track your Amazon Route 53 costs. When you apply tags to Route 53 hosted zones, domains, and health checks, AWS generates a cost allocation report as a comma-separated value (CSV) file with your usage and costs aggregated by your tags. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple services. For more information about using tags for cost allocation, see [Using cost allocation tags](#) in the [AWS Billing and Cost Management User Guide](#).

For ease of use and best results, use Tag Editor in the AWS Management Console, which provides a central, unified way to create and manage your tags. For more information, see [Working with Tag Editor](#) in [Getting Started with the AWS Management Console](#). You can also use the Route 53 console to apply tags for some resources:

- **Health checks** – For more information, see [Naming and tagging health checks \(p. 551\)](#).
- **Route 53 Resolver inbound endpoints** – For more information, see [Values that you specify when you create or edit inbound endpoints \(p. 482\)](#).
- **Resolver outbound endpoints** – For more information, see [Values that you specify when you create or edit outbound endpoints \(p. 484\)](#).
- **Resolver rules** – For more information, see [Values that you specify when you create or edit rules \(p. 485\)](#).

Note

Charges for Resolver are based in part on VPC elastic network interfaces, which correspond with the IP addresses that you specify for inbound and outbound endpoints. You can't currently tag elastic network interfaces that are created by Resolver, so you can't use tags for allocating costs for Resolver. For information about pricing for Resolver, see [Amazon Route 53 pricing](#).

You can also apply tags to resources by using the Route 53 API. For more information, see the actions related to tags in the topic [Route 53 API actions by function](#) in the [Amazon Route 53 API Reference](#).

Tutorials

The following tutorials explain how to use Amazon Route 53 as the DNS service for a subdomain while still using another DNS service for the domain and how to use Route 53 for several use cases related to weighted and latency records.

Topics

- [Using Amazon Route 53 as the DNS service for subdomains without migrating the parent domain \(p. 656\)](#)
- [Transitioning to latency-based routing in Amazon Route 53 \(p. 661\)](#)
- [Adding another Region to your latency-based routing in Amazon Route 53 \(p. 662\)](#)
- [Using latency and weighted records in Amazon Route 53 to route traffic to multiple Amazon EC2 instances in a Region \(p. 664\)](#)
- [Managing over 100 weighted records in Amazon Route 53 \(p. 664\)](#)
- [Weighting fault-tolerant multi-record answers in Amazon Route 53 \(p. 665\)](#)

Using Amazon Route 53 as the DNS service for subdomains without migrating the parent domain

You can use Amazon Route 53 as the DNS service for a new subdomain or an existing subdomain and still use another DNS service for the parent domain. For more information, see the applicable topic.

Topics

- [Creating a subdomain that uses Amazon Route 53 as the DNS service without migrating the parent domain \(p. 656\)](#)
- [Migrating DNS service for a subdomain to Amazon Route 53 without migrating the parent domain \(p. 658\)](#)

Creating a subdomain that uses Amazon Route 53 as the DNS service without migrating the parent domain

You can create a subdomain that uses Amazon Route 53 as the DNS service without migrating the parent domain from another DNS service.

The process has the following basic steps:

1. [Figure out \(p. 657\) whether you should even be using this procedure.](#)
2. [Create a Route 53 hosted zone for the subdomain \(p. 657\).](#)
3. [Add records \(p. 657\) for the new subdomain to your Route 53 hosted zone.](#)
4. [API only: Confirm that your changes have propagated \(p. 657\) to all Route 53 DNS servers.](#)

Note

Currently, the only way to verify that changes have propagated is to use the [GetChange](#) API action. Changes generally propagate to all Route 53 name servers within 60 seconds.

5. [Update the DNS service for the parent domain by adding name server records for the subdomain \(p. 657\).](#)

Deciding which procedures to use for creating a subdomain

The procedures in this topic explain how to perform an uncommon operation. If you're already using Route 53 as the DNS service for your domain and you just want to route traffic for a subdomain, such as `www.example.com`, to your resources, such as a web server running on an EC2 instance, see [Routing traffic for subdomains \(p. 335\)](#).

Use this procedure *only* if you're using another DNS service for a domain, such as `example.com`, and you want to start using Route 53 as the DNS service for a new subdomain of that domain, such as `www.example.com`.

Creating a hosted zone for the new subdomain

When you want to use Amazon Route 53 as the DNS service for a new subdomain without migrating the parent domain, you start by creating a hosted zone for the subdomain. Route 53 stores information about your subdomain in the hosted zone.

For information about how to create a hosted zone using the Route 53 console, see [Creating a public hosted zone \(p. 340\)](#).

Creating records

You can create records using either the Amazon Route 53 console or the Route 53 API. The records that you create in Route 53 will become the records that DNS uses after you delegate responsibility for the subdomain to Route 53, as explained in [Updating your DNS service with name server records for the subdomain \(p. 657\)](#), later in the process.

Important

Do not create additional name server (NS) or start of authority (SOA) records in the Route 53 hosted zone, and do not delete the existing NS and SOA records.

To create records using the Route 53 console, see [Working with records \(p. 370\)](#). To create records using the Route 53 API, use `ChangeResourceRecordSets`. For more information, see `ChangeResourceRecordSets` in the [Amazon Route 53 API Reference](#).

Checking the status of your changes (API only)

Creating a new hosted zone and changing records take time to propagate to the Route 53 DNS servers. If you used `ChangeResourceRecordSets` to create your records, you can use the `GetChange` action to determine whether your changes have propagated. (`ChangeResourceRecordSets` returns a value for `ChangeId`, which you can include in a subsequent `GetChange` request. `ChangeId` is not available if you created the records by using the console.) For more information, see [GET GetChange](#) in the [Amazon Route 53 API Reference](#).

Note

Changes generally propagate to all Route 53 name servers within 60 seconds.

Updating your DNS service with name server records for the subdomain

After your changes to Amazon Route 53 records have propagated (see [Checking the status of your changes \(API only\) \(p. 657\)](#)), update the DNS service for the parent domain by adding NS records for the subdomain. This is known as delegating responsibility for the subdomain to Route 53. For example, if the parent domain `example.com` is hosted with another DNS service and you created the subdomain `test.example.com` in Route 53, you must update the DNS service for `example.com` with new NS records for `test.example.com`.

Perform the following procedure.

1. Using the method provided by your DNS service, back up the zone file for the parent domain.
2. In the Route 53 console, get the name servers for your Route 53 hosted zone:
 - a. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 - b. In the navigation pane, click **Hosted zones**.
 - c. On the **Hosted zones** page, choose the radio button (not the name) for the hosted zone, then choose **View details**.
 - d. On the details page for the hosted zone, choose **Hosted zone details**.
 - e. Make note of the four servers listed for **Name servers**.
- Alternatively, you can use the `GetHostedZone` action. For more information, see [GetHostedZone](#) in the *Amazon Route 53 API Reference*.
3. Using the method provided by the DNS service of the parent domain, add NS records for the subdomain to the zone file for the parent domain. In these NS records, specify the four Route 53 name servers that are associated with the hosted zone that you created in Step 1.

Important

Do not add a start of authority (SOA) record to the zone file for the parent domain. Because the subdomain will use Route 53, the DNS service for the parent domain is not the authority for the subdomain.

If your DNS service automatically added an SOA record for the subdomain, delete the record for the subdomain. However, do not delete the SOA record for the parent domain.

Migrating DNS service for a subdomain to Amazon Route 53 without migrating the parent domain

You can migrate a subdomain to use Amazon Route 53 as the DNS service without migrating the parent domain from another DNS service.

The process has the following basic steps:

1. [Figure out \(p. 658\)](#) whether you should even be using this procedure.
2. [Create a Route 53 hosted zone for the subdomain \(p. 659\)](#).
3. [Get the current DNS configuration from the current DNS service provider for the parent domain \(p. 659\)](#).
4. [Add records \(p. 659\)](#) for the subdomain to your Route 53 hosted zone.
5. [API only: Confirm that your changes have propagated \(p. 659\)](#) to all Route 53 DNS servers.

Note

Currently, the only way to verify that changes have propagated is to use the [GetChange](#) API action. Changes generally propagate to all Route 53 name servers within 60 seconds.

6. [Update the DNS configuration with the DNS service provider for the parent domain by adding name server records for the subdomain \(p. 660\)](#).

Deciding which procedures to use for creating a subdomain

The procedures in this topic explain how to perform an uncommon operation. If you're already using Route 53 as the DNS service for your domain and you just want to route traffic for a subdomain, such as `www.example.com`, to your resources, such as a web server running on an EC2 instance, see [Routing traffic for subdomains \(p. 335\)](#).

Use this procedure *only* if you're using another DNS service for a domain, such as example.com, and you want to start using Route 53 as the DNS service for an existing subdomain of that domain, such as www.example.com.

Creating a hosted zone for the subdomain

If you want to migrate a subdomain from another DNS service to Amazon Route 53 but you don't want to migrate the parent domain, start by creating a hosted zone for the subdomain. Route 53 stores information about your subdomain in the hosted zone.

For information about how to create a hosted zone using the Route 53 console, see [Creating a public hosted zone \(p. 340\)](#).

Getting your current DNS configuration from your DNS service provider

To simplify the process of migrating an existing subdomain to Route 53, get the current DNS configuration for the domain from the DNS service provider that is currently servicing the domain. You can use this information as a basis for configuring Route 53 as the DNS service for the subdomain.

What you ask for and the format that it comes in depends on which company you're currently using as your DNS service provider. Ideally, they'll give you a zone file, which contains information about all of the records in your current configuration. (Records tell DNS how you want traffic to be routed for your domains and subdomains. For example, when someone enters your domain name in a web browser, do you want traffic to be routed to a web server in your data center, to an Amazon EC2 instance, to a CloudFront distribution, or to some other location?) If you can get a zone file from your current DNS service provider, you can edit the zone file to remove the records that you don't want to migrate to Amazon Route 53. Then you can import the remaining records into your Route 53 hosted zone, which greatly simplifies the process. Try asking customer support for your current DNS service provider how to get a *zone file* or a *records list*.

Creating records

Using the records that you got from your current DNS service provider as a starting point, create corresponding records in the Amazon Route 53 hosted zone that you created for the subdomain. The records that you create in Route 53 will become the records that DNS uses after you delegate responsibility for the subdomain to Route 53, as explained in [Updating your DNS service with name server records for the subdomain \(p. 660\)](#), later in the process.

Important

Do not create additional name server (NS) or start of authority (SOA) records in the Route 53 hosted zone, and do not delete the existing NS and SOA records.

To create records using the Route 53 console, see [Working with records \(p. 370\)](#). To create records using the Route 53 API, use `ChangeResourceRecordSets`. For more information, see `ChangeResourceRecordSets` in the [Amazon Route 53 API Reference](#).

Checking the status of your changes (API only)

Creating a new hosted zone and changing records take time to propagate to the Route 53 DNS servers. If you used `ChangeResourceRecordSets` to create your records, you can use the `GetChange` action to determine whether your changes have propagated. (`ChangeResourceRecordSets` returns a value for `ChangeId`, which you can include in a subsequent `GetChange` request. `ChangeId` is not available if you created the records by using the console.) For more information, see [GET GetChange](#) in the [Amazon Route 53 API Reference](#).

Note

Changes generally propagate to all Route 53 name servers within 60 seconds.

Updating your DNS service with name server records for the subdomain

After your changes to Amazon Route 53 records have propagated (see [Checking the status of your changes \(API only\) \(p. 659\)](#)), update the DNS service for the parent domain by adding NS records for the subdomain. This is known as delegating responsibility for the subdomain to Route 53. For example, suppose the parent domain example.com is hosted with another DNS service and you're migrating the subdomain test.example.com to Route 53. You must create a hosted zone for test.example.com and update the DNS service for example.com with the NS records that Route 53 assigned to the new hosted zone for test.example.com.

Perform the following procedure.

1. Using the method provided by your DNS service, back up the zone file for the parent domain.
2. If the previous DNS service provider for the domain has a method to change the TTL settings for their name servers, we recommend that you change the settings to 900 seconds. This limits the time during which client requests will try to resolve domain names using obsolete name servers. If the current TTL is 172800 seconds (two days), which is a common default setting, you still need to wait two days for resolvers and clients to stop caching DNS records using the previous TTL. After the TTL settings expire, you can safely delete the records that are stored at the previous provider and make changes only to Route 53.
3. In the Route 53 console, get the name servers for your Route 53 hosted zone:
 - a. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
 - b. In the navigation pane, click **Hosted zones**.
 - c. On the **Hosted zones** page, choose the radio button (not the name) for the hosted zone, then choose **View details**.
 - d. On the details page for the hosted zone, choose **Hosted zone details**.
 - e. Make note of the four servers listed for **Name servers**.

Alternatively, you can use the `GetHostedZone` action. For more information, see [GetHostedZone](#) in the *Amazon Route 53 API Reference*.

4. Using the method provided by the DNS service of the parent domain, add NS records for the subdomain to the zone file for the parent domain. Give the NS records the same name as the subdomain. For the values in the NS records, specify the four Route 53 name servers that are associated with the hosted zone that you created in Step 2. Note that different DNS services use different terminology. You might need to contact technical support for your DNS service to learn how to perform this step.

Important

Do not add a start of authority (SOA) record to the zone file for the parent domain. Because the subdomain will use Route 53, the DNS service for the parent domain is not the authority for the subdomain.

If your DNS service automatically added an SOA record for the subdomain, delete the record for the subdomain. However, do not delete the SOA record for the parent domain.

Depending on the TTL settings for the name servers for the parent domain, the propagation of your changes to DNS resolvers can take 48 hours or more. During this period, DNS resolvers may still answer requests with the name servers for the DNS service of the parent domain. In addition, client computers may continue to have the previous name servers for the subdomain in their cache.

5. After the registrar's TTL settings for the domain expire (see Step 2), delete the following records from the zone file for the parent domain:
 - The records that you added to Route 53 as described in [Creating records \(p. 659\)](#).

- Your DNS service's NS records. When you are finished deleting NS records, the only NS records in the zone file will be the ones that you created in Step 4.

Transitioning to latency-based routing in Amazon Route 53

With latency-based routing, Amazon Route 53 can direct your users to the lowest-latency AWS endpoint available. For example, you might associate a DNS name like `www.example.com` with an ELB Classic, Application, or Network Load Balancer, or with Amazon EC2 instances or Elastic IP addresses that are hosted in the US East (Ohio) and Europe (Ireland) regions. The Route 53 DNS servers decide, based on network conditions of the past couple of weeks, which instances in which regions should serve particular users. A user in London will likely be directed to the Europe (Ireland) instance, a user in Chicago will likely be directed to the US East (Ohio) instance, and so on. Route 53 supports latency-based routing for A, AAAA, TXT, and CNAME records, as well as aliases to A and AAAA records.

Note

Data about the latency between users and your resources is based entirely on traffic between users and AWS data centers. If you aren't using resources in an AWS Region, the actual latency between your users and your resources can vary significantly from AWS latency data. This is true even if your resources are located in the same city as an AWS Region.

For a smooth, low-risk transition, you can combine weighted and latency records to gradually migrate from standard routing to latency-based routing with full control and rollback capability at each stage. Let's consider an example in which `www.example.com` is currently hosted on an Amazon EC2 instance in the US East (Ohio) region. The instance has the Elastic IP address `w.w.w.w`. Suppose you want to continue routing traffic to the US East (Ohio) region when applicable while also beginning to direct users to additional Amazon EC2 instances in the US West (N. California) region (Elastic IP `x.x.x.x`) and in the Europe (Ireland) region (Elastic IP `y.y.y.y`). The Route 53 hosted zone for `example.com` already has a record for `www.example.com` that has a **Type** of A and a **Value** (an IP address) of `w.w.w.w`.

When you're finished with the following example, you'll have two weighted alias records:

- You'll convert your existing record for `www.example.com` into a weighted alias record that continues to direct the majority of your traffic to your existing Amazon EC2 instance in the US East (Ohio) region.
- You'll create another weighted alias record that initially directs only a small portion of your traffic to your latency records, which route traffic to all three regions.

By updating the weights in these weighted alias records, you can gradually shift from routing traffic only to the US East (Ohio) region to routing traffic to all three regions in which you have Amazon EC2 instances.

To transition to latency-based routing

1. Make a copy of the record for `www.example.com`, but use a new domain name, for example, `copy-www.example.com`. Give the new record the same **Type** (A) and **Value** (`w.w.w.w`) as the record for `www.example.com`.
2. Update the existing A record for `www.example.com` to make it a weighted alias record:
 - For **Value/Route traffic to**, choose **Alias to another record in this hosted zone**, and specify `copy-www.example.com`.
 - For **Weight**, specify 100.

When you're finished with the update, Route 53 will continue to use this record to route all traffic to the resource that has an IP address of `w.w.w.w`.

3. Create a latency record for each of your Amazon EC2 instances, for example:

- US East (Ohio), Elastic IP address `w.w.w.w`
- US West (N. California), Elastic IP address `x.x.x.x`
- Europe (Ireland), Elastic IP address `y.y.y.y`

Give all of the latency records the same domain name, for example, `www-lbr.example.com` and the same type, A.

When you're finished creating the latency records, Route 53 will continue to route traffic using the record that you updated in Step 2.

You can use `www-lbr.example.com` for validation testing, for example, to ensure that each endpoint can accept requests.

4. Let's now add the `www-lbr.example.com` latency record into the `www.example.com` weighted record and begin routing limited traffic to the corresponding Amazon EC2 instances. This means that the Amazon EC2 instance in the US East (Ohio) region will be getting traffic from both weighted records.

Create another weighted alias record for `www.example.com`:

- For **Value/Route traffic to**, choose **Alias to another record in this hosted zone**, and specify `www-lbr.example.com`.
- For **Weight**, specify 1.

When you finish and your changes are synchronized to Route 53 servers, Route 53 will begin to route a tiny fraction of your traffic (1/101) to the Amazon EC2 instances for which you created latency records in Step 3.

5. As you develop confidence that your endpoints are adequately scaled for the incoming traffic, adjust the weights accordingly. For example, if you want 10% of your requests to be based on latency-based routing, change the weights to 90 and 10, respectively.

For more information about creating latency records, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

Adding another Region to your latency-based routing in Amazon Route 53

If you're using latency based routing and you want to add an instance in a new region, you can gradually shift traffic to the new region in the same way that you gradually shifted traffic to latency-based routing in [Transitioning to latency-based routing in Amazon Route 53 \(p. 661\)](#).

For example, suppose you're using latency-based routing to route traffic for `www.example.com`, and you want to add an Amazon EC2 instance in Asia Pacific (Tokyo) to your instances in US East (Ohio), US West (N. California), and Europe (Ireland). The following example procedure explains one way that you could add an instance in another region.

For this example, the Amazon Route 53 hosted zone for `example.com` already has a weighted alias record for `www.example.com` that is routing traffic to the latency-based records for `www-lbr.example.com`:

- US East (Ohio), Elastic IP address `w.w.w.w`

- US West (N. California), Elastic IP address X.X.X.X
- Europe (Ireland), Elastic IP address Y.Y.Y.Y

The weighted alias record has a weight of 100. After you transitioned to latency-based routing, assume that you deleted the other weighted record that you used for the transition.

To add another Region to your latency-based routing in Route 53

1. Create four new latency-based records that include the three original regions as well as the new region to which you want to start routing traffic.
 - US East (Ohio), Elastic IP address W.W.W.W
 - US West (N. California), Elastic IP address X.X.X.X
 - Europe (Ireland), Elastic IP address Y.Y.Y.Y
 - Asia Pacific (Tokyo), Elastic IP address Z.Z.Z.Z

Give all of the latency records the same new domain name, for example, `www-1br-2012-04-30.example.com`, and the same type, A.

When you're finished creating the latency records, Route 53 will continue to route traffic using the original weighted alias record (`www.example.com`) and latency records (`www-1br.example.com`).

You can use the `www-1br-2012-04-30.example.com` records for validation testing, for example, to ensure that each endpoint can accept requests.

2. Create a weighted alias record for the new latency records:
 - For the domain name, specify the name for the existing weighted alias record, `www.example.com`.
 - For **Value/Route traffic to**, choose **Alias to another record in this hosted zone**, and specify `www-1br-2012-04-30.example.com`.
 - For **Weight**, specify 1.

When you finish, Route 53 will begin to route a tiny fraction of your traffic (1/101) to the Amazon EC2 instances for which you created the `www-1br-2012-04-30.example.com` latency records in Step 1. The remainder of the traffic will continue to be routed to the `www-1br.example.com` latency records, which do not include the Amazon EC2 instance in the Asia Pacific (Tokyo) region.

3. As you develop confidence that your endpoints are adequately scaled for the incoming traffic, adjust the weights accordingly. For example, if you want 10% of your requests to be routed to the latency records that include the Tokyo region, change the weight for `www-1br.example.com` from 100 to 90 and the weight for `www-1br-2012-04-30.example.com` from 1 to 10.

For more information about creating records, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

Using latency and weighted records in Amazon Route 53 to route traffic to multiple Amazon EC2 instances in a Region

If your application is running on Amazon EC2 instances in two or more Amazon EC2 regions, and if you have more than one Amazon EC2 instance in one or more regions, you can use latency-based routing to route traffic to the correct region and then use weighted records to route traffic to instances within the region based on weights that you specify.

For example, suppose you have three Amazon EC2 instances with Elastic IP addresses in the US East (Ohio) region and you want to distribute requests across all three IPs evenly for users for whom US East (Ohio) is the appropriate region. Just one Amazon EC2 instance is sufficient in the other regions, although you can apply the same technique to many regions at once.

To use latency and weighted records in Amazon Route 53 to route traffic to multiple Amazon EC2 instances in a region

1. Create a group of weighted records for the Amazon EC2 instances in the region. Note the following:
 - Give each weighted record the same value for **Record name** (for example, `us-east.example.com`) and **Record type**.
 - For **Value/Route traffic to**, choose **IP address or another value depending on the record type**, and specify the value of one of the Elastic IP addresses.
 - If you want to weight the Amazon EC2 instances equally, specify the same value for **Weight**.
 - Specify a unique value for **Set ID** for each record.

For more information about weighted record values, see [Weighted routing \(p. 378\)](#)

2. If you have multiple Amazon EC2 instances in other regions, repeat Step 1 for the other regions. Specify a different value for **Name** in each region.
3. For each region in which you have multiple Amazon EC2 instances (for example, US East (Ohio)), create a latency alias record. For **Value/Route traffic to**, choose **Alias to another record in this hosted zone**, and specify the value of the **Record name** field (for example, `us-east.example.com`) that you assigned to the weighted records in that region.
4. For each region in which you have one Amazon EC2 instance, create a latency record. For **Record name**, specify the same value that you specified for the latency alias records that you created in Step 3. For **Value/Route traffic to**, choose **IP address or another value depending on the record type**, and specify the Elastic IP address of the Amazon EC2 instance in that Region.

For more information about adding alias records to Amazon EC2 instances, see [Routing traffic to an Amazon EC2 instance \(p. 500\)](#)

For more information about creating records, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#).

Managing over 100 weighted records in Amazon Route 53

Amazon Route 53 lets you configure weighted records. For a given name and type (for example, `www.example.com`, type A), you can configure up to 100 alternative responses, each with its own

weight. When responding to queries for `www.example.com`, Route 53 DNS servers select a weighted random response to return to DNS resolvers. The value of a weighted record that has a weight of 2 is returned, on average, twice as often as the value of a weighted record that has a weight of 1.

If you need to direct traffic to more than 100 endpoints, one way to achieve this is to use a tree of weighted alias records and weighted records. For example, the first "level" of the tree may be up to 100 weighted alias records, each of which can, in turn, point to up to 100 weighted records. Route 53 permits up to three levels of recursion, allowing you to manage up to 1,000,000 unique weighted endpoints.

A simple two-level tree might look like this:

Weighted alias records

- `www.example.com` aliases to `www-a.example.com` with a weight of 1
- `www.example.com` aliases to `www-b.example.com` with a weight of 1

Weighted records

- `www-a.example.com`, type A, value 192.0.2.1, weight 1
- `www-a.example.com`, type A, value 192.0.2.2, weight 1
- `www-b.example.com`, type A, value 192.0.2.3, weight 1
- `www-b.example.com`, type A, value 192.0.2.4, weight 1

For more information about creating records, see [Working with records \(p. 370\)](#).

Weighting fault-tolerant multi-record answers in Amazon Route 53

Note

Records that use the multivalue answer routing policy behave in much the same way as the configuration that is documented in this tutorial. The main difference is that the tutorial configuration lets you specify weights, which can be useful when your endpoints have different capacities. For more information, see [Multivalue answer routing \(p. 378\)](#).

An Amazon Route 53 weighted record can only be associated with one record, meaning a combination of one name (for example, `example.com`) and one record type (for example, A). But it is often desirable to weight DNS responses that contain multiple records.

For example, you might have eight Amazon EC2 instances or Elastic IP endpoints for a service. If the clients of that service support connection retries (as all common browsers do), then providing multiple IP addresses in DNS responses provides those clients with alternative endpoints in the event of the failure of any particular endpoint. You can even protect against the failure of an availability zone if you configure responses to contain a mix of IPs hosted in two or more availability zones.

Multi-record answers are also useful when a large number of clients (for example, mobile web applications) share a small set of DNS caches. In this case, multi-record answers allow clients to direct requests to several endpoints even if they receive a common DNS response from the shared cache.

These types of weighted multi-record answers can be achieved by using a combination of records and weighted alias records. You can group eight endpoints into two distinct record sets containing four IP addresses each:

`endpoint-a.example.com`, type A, with the following values:

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, type A, with the following values:

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

You can then create a weighted alias record that points to each group:

- `www.example.com` aliases to `endpoint-a.example.com`, type A, weight 1
- `www.example.com` aliases to `endpoint-b.example.com`, type A, weight 1

For more information about creating records, see [Working with records \(p. 370\)](#).

Best practices for Amazon Route 53

Follow these best practices when you configure Route 53.

Topics

- [Best practices for Amazon Route 53 DNS \(p. 667\)](#)
- [Best practices for Resolver \(p. 668\)](#)
- [Best practices for Amazon Route 53 health checks \(p. 670\)](#)

Best practices for Amazon Route 53 DNS

Follow these best practices to get the best results when using Route 53 DNS service.

Use the data plane functions for DNS failover and app recovery

The data planes for Route 53, including health checks, and Amazon Route 53 Application Recovery Controller routing control are globally distributed, and are designed for 100% availability and functionality, even during severe events. They integrate with each other and don't depend on control plane functionality. While the control planes for these services, including their consoles, are generally very reliable, they're designed in a more centralized way and prioritize durability and consistency rather than high availability. For scenarios such as failover during disaster recovery, we recommend that you use features like Route 53 health checks and Route 53 ARC that rely on data plane functionality to update DNS. For more information, see [Creating Disaster Recovery Mechanisms Using Amazon Route 53](#).

Choosing TTL values for DNS records

The DNS TTL is the numeric value (in seconds) that DNS resolvers use to decide how long a record may be cached for without making another query to Route 53. All DNS records must specify a TTL. The recommended range for TTL values is 60 to 172,800 seconds.

The choice of a TTL is a trade-off between latency and reliability, and responsiveness to change. With shorter TTLs on a record, DNS resolvers will notice updates to the record quicker as they must query more frequently. This will increase the query volume (and cost). As you lengthen the TTL, DNS resolvers answer queries from cache more often which is typically faster, cheaper, and in some situations more reliable because it avoids queries across the internet. There is no correct value, but it is worthwhile to think about whether responsiveness or reliability is more important to you.

Things to consider while setting TTL values:

- Set DNS record TTLs as long as you can afford to wait for a change to take effect. This is especially true on delegations (NS recordsets), or other records that rarely change, for example MX records. For these records longer TTLs are preferred. Between an hour (3600s) or a day (86,400s) is a common choice.
- For records that need to be altered as part of a rapid failover mechanism (especially records that are health checked), lower TTLs are appropriate. 60 or 120 seconds are common choices.
- When you make changes to critical DNS entries, it is advisable to temporarily shorten the TTLs, so that you can make the change, observe and then rollback quickly if you need to. Once the change is in place and working as expected, you can raise the TTL to a longer value.

For more information see [TTL \(seconds\) \(p. 395\)](#).

CNAME records

CNAME records in DNS are a way to point one domain name at another. If a DNS resolver resolves domain-1.example.com and finds a CNAME pointing at domain-2.example.com, the DNS resolver must proceed to resolve domain-2.example.com before it can respond. These records are useful in many situations, for example, to ensure consistency when a website has more than one domain name.

However, DNS resolvers must make more queries to answer CNAMEs, which increases latency and costs. Where possible, a faster and cheaper alternative is to use a Route 53 ALIAS record. Aliases allow Route 53 to respond with the direct answer for AWS resources (for example, Elastic Load Balancing) and for other domains within the same hosted zone.

For more information, see [Routing internet traffic to your AWS resources \(p. 496\)](#).

Advanced DNS routing

- When using geolocation, geoproximity or latency-based routing, always set a default, unless you want some clients to receive *no answer* responses.
- To minimize application latency, use latency-based routing. This type of routing data can change frequently.
- To provide routing stability and predictability, use either geolocation or geoproximity routing.

For more information, see [Geolocation routing \(p. 372\)](#), [Geoproximity routing \(traffic flow only\) \(p. 373\)](#), and [Latency-based routing \(p. 377\)](#).

Confirm DNS changes.

When you create or update a record by using the Route 53 console or API, it takes some time for the change to be reflected across the internet. This is called *change propagation*. While propagation is typically under one minute globally, there're occasionally cases where a change can be delayed, for example, due to problems syncing to one location, or in rare cases, problems within the central control plane. Use the [GetChange](#) API to verify your DNS changes have gone into effect (`Status =INSYNC`) if you are building automated provisioning work flows, and it is important to wait for change propagation to complete before moving forward with the next work flow step.

DNS delegation

When you delegate multiple levels of subdomains in DNS, it is important to always delegate from the parent zone. For example, if you are delegating www.dept.example.com you should do so from the dept.example.com zone, not from the example.com zone. Delegations from a *grandparent* to a *child* zone may not work at all or work only inconsistently. For more information, see [Routing traffic for subdomains \(p. 335\)](#).

Size of DNS response

Avoid creating large single responses. Above 512 bytes, many DNS resolvers must retry over TCP instead of UDP, which can lead to slower responses and reduced reliability. We recommend using multi-value answers which chooses 8 healthy, random IPs to keep responses within the 512 byte boundary.

For more information, see [Multivalue answer routing \(p. 378\)](#) and [DNS Reply Size Test Server](#).

Best practices for Resolver

Follow these best practices for optimizing Route 53 Resolver.

Topics

- [Avoid loop configurations with Resolver endpoints \(p. 669\)](#)
- [Resolver endpoint scaling \(p. 669\)](#)
- [High availability for Resolver endpoints \(p. 669\)](#)

- [DNS zone walking \(p. 670\)](#)

Avoid loop configurations with Resolver endpoints

Don't associate the same VPC to a Resolver rule and its inbound endpoint (whether it's a direct target of the endpoint, or via an on-premises DNS server). When the outbound endpoint in a Resolver rule points to an inbound endpoint that shares a VPC with the rule, it can cause a loop where the query is continually passed between the inbound and outbound endpoints.

The forwarding rule can still be associated with other VPCs that are shared with other accounts by using AWS Resource Access Manager (AWS RAM). Private hosted zones associated with the hub, or a central VPC, will still resolve from queries to inbound endpoints because a forwarding resolver rule does not change this resolution.

Resolver endpoint scaling

Resolver endpoint security groups use connection tracking to gather information about traffic to and from the endpoints. Each endpoint interface has a maximum number of connections that can be tracked, and a high volume of DNS queries can exceed the connections and cause throttling and query loss. To reduce the number of connections that are tracked, implement security group rules that permit traffic based on the connection state of the traffic. For more information, see [Security groups](#) and [Connection tracking](#) in *Amazon EC2 User Guide for Linux Instances*.

Inbound and Outbound Resolver security group recommendations

Inbound rules		
Protocol type	Port number	Source IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0
Outbound rules		
Protocol type	Port number	Destination IP
TCP	All	0.0.0.0/0
UDP	All	0.0.0.0/0

Inbound Resolver endpoints

For clients using an inbound resolver endpoint, the capacity of the elastic network interface will be impacted if you have over 40,000 unique IP address and port combinations generating the DNS traffic.

High availability for Resolver endpoints

When you create your Route 53 Resolver inbound endpoints, Route 53 requires that you create at least two IP addresses that the DNS resolvers on your network will forward queries to. You should also specify IP addresses in at least two Availability Zones for redundancy.

If you require more than one elastic network interface endpoint to be available at all times, we recommend that you create at least one more network interface than you need, to make sure you have additional capacity available for handling possible traffic surges. The additional network interface also ensures availability during service operations like maintenance or upgrades.

For more information, see [Values that you specify when you create or edit inbound endpoints \(p. 482\)](#).

DNS zone walking

A DNS zone walking attack attempts to get all content from DNSSEC-signed DNS zones. If Route 53 Resolver team detects a traffic pattern that matches the ones generated when DNS zones are walked on your endpoint, the service team will throttle the traffic on your endpoint. As a consequence you might observe a high percentage of your DNS queries timing out.

If you observe reduced capacity on your endpoints and believe that the endpoint have been throttled erroneously, go to <https://console.aws.amazon.com/support/home#/> to create a support case.

Best practices for Amazon Route 53 health checks

Follow these best practices for optimizing Amazon Route 53 health checks.

Topics

- [Best practices for Elastic IP addresses for health checks \(p. 670\)](#)

Best practices for Elastic IP addresses for health checks

Best practice for your health check endpoints is to use Elastic IP addresses. However, be sure to delete any health check that is associated with an Elastic IP address that you no longer own. For example, if you are no longer using an Amazon EC2 instance, make sure you delete any health check that is associated to its Elastic IP address. This is because the Elastic IP address can be assigned to a different user or AWS account, which might compromise your health check data.

Quotas

Amazon Route 53 API requests and entities are subject to the following quotas (formerly referred to as "limits").

Topics

- [Using Service Quotas to view and manage quotas \(p. 671\)](#)
- [Quotas on entities \(p. 671\)](#)
- [Maximums on API requests \(p. 675\)](#)

Using Service Quotas to view and manage quotas

You can use the Service Quotas service to view quotas and to request quota increases for many AWS services. For more information, see the [Service Quotas User Guide](#). (You can currently use Service Quotas to view and manage only Route 53 and Route 53 Resolver quotas. Domain registration quotas aren't available.)

Note

To view quotas and request higher quotas for Route 53, you must change the Region to US East (N. Virginia). To view quotas and request higher quotas for Resolver, change to the applicable Region.

Quotas on entities

Amazon Route 53 entities are subject to the following quotas.

For information on getting current quotas (formerly referred to as "limits"), see the following Route 53 actions:

- [GetAccountLimit](#) – Gets quotas on health checks, hosted zones, reusable delegation sets, traffic flow policies, and traffic flow policy records
- [GetHostedZoneLimit](#) – Gets quotas on records in a hosted zone and on Amazon VPCs that you can associate with a private hosted zone
- [GetReusableDelegationSetLimit](#) – Gets the quota on the number of hosted zones that you can associate with a reusable delegation set

Topics

- [Quotas on domains \(p. 672\)](#)
- [Quotas on hosted zones \(p. 672\)](#)
- [Quotas on records \(p. 672\)](#)
- [Quotas on Route 53 Resolver \(p. 673\)](#)
- [Quotas on health checks \(p. 675\)](#)
- [Quotas on query log configurations \(p. 675\)](#)
- [Quotas on traffic flow policies and policy records \(p. 675\)](#)
- [Quotas on reusable delegation sets \(p. 675\)](#)

Quotas on domains

Entity	Quota
Domains	20* per AWS account Request a higher quota.

*The limit is 20 for new customers as of March 2021.

If you have an existing account and your default limit is 50 now, it will remain at 50.

Quotas on hosted zones

Entity	Quota
Hosted zones	500 per AWS account Request a higher quota.
Hosted zones that can use the same reusable delegation set	100 Request a higher quota.
Amazon VPCs that you can associate with a private hosted zone per hosted zone	300 Request a higher quota.
Private hosted zones that you can associate a VPC with	No quota *
Authorizations that you can create so you can associate VPCs that were created by one account with a hosted zone that was created by another account	100
The number of key signing keys (KSK) that you can create per hosted zone	2

* You can associate a VPC with any or all of the private hosted zones that you control through your AWS accounts. For example, suppose you have three AWS accounts and all three have the default quota of 500 hosted zones. If you create 500 private hosted zones for all three accounts, you can associate a VPC with all 1,500 private hosted zones.

Quotas on records

Entity	Quota
Records	10,000 per hosted zone Request a higher quota.

Entity	Quota
	For a quota greater than 10,000 records in a hosted zone, an additional charge applies. For more information, see Amazon Route 53 Pricing .
Values in a record	400 per record
Geolocation, latency, multivalue answer, and weighted records	100 records that have the same name and type
Geoproximity records	30 records that have the same name and type

Quotas on Route 53 Resolver

This section includes all the Route 53 Resolver quotas.

Quotas on Route 53 Resolver

Use the following procedure to increase quotas for Route 53 Resolver.

To increase Resolver quotas

1. Open the Service Quotas console at <https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas>.
2. Go to the region where you want to increase the limit.
3. Select the Route 53 Resolver **Quota name** you want to increase.
4. Select **Request quota increase**, enter the quota value, and then select **Request**.

Quotas on Route 53 Resolver endpoints

Entity	Quota
Endpoints per AWS Region	4 per AWS account Request a higher quota (p. 673) .
IP addresses per endpoint	6 Request a higher quota (p. 673) .
IP addresses per rule	6
Rules per AWS Region	1000 per AWS account Request a higher quota (p. 673) .
Associations between rules and VPCs per AWS Region	2000 per AWS account Request a higher quota (p. 673) .
Queries per second per IP address in an endpoint	10,000*

* Each elastic network interface endpoint can process up to 10,000 DNS queries per second (QPS). The number of DNS QPS varies by the type of query, size of the response, health of the target name servers, query response times, round trip latency, and the protocol in use. For example, queries to a target name server that is slow to respond can significantly reduce the capacity of the network interface. Additionally, to ensure high availability, Route 53 Resolver generates redundant outbound queries for each DNS request that it receives. As a result, the QPS for each outbound network interface will not match the QPS sent to Route 53 Resolver. Use CloudWatch metrics to measure how many queries are being sent to each network interface. For more information, see [Metrics for Resolver IP addresses \(p. 632\)](#). If your maximum query rate exceeds 50% of the capacity for any network interface in the endpoint, you can add more network interfaces to increase the endpoint capacity.

Quotas on Route 53 Resolver query logs

Entity	Quota
Query log configurations per AWS Region	20
Query log configuration VPC associations per AWS Region	100
Query log configuration VPC associations per AWS Region (shared using RAM)	100

Quotas on Route 53 Resolver DNS Firewall

Entity	Quota
Number of rule groups associated to a VPC for a single account per AWS Region	5
Number of DNS Firewall domains in a single Amazon S3 file for a single account per AWS Region	100,000 Request a higher quota (p. 673).
Number of DNS Firewall rule groups for a single account per AWS Region	1,000 Request a higher quota (p. 673).
Number of rules within a rule group for a single account account per AWS Region	100 Request a higher quota (p. 673).
Number of domain lists for a single account account per AWS Region	1000 Request a higher quota (p. 673).
Number of domain specifications across all DNS Firewall domain lists for a single account per AWS Region	100,000 Request a higher quota (p. 673).

Quotas on health checks

Entity	Quota
Health checks	200 active health checks per AWS account Request a higher quota.
Child health checks that a calculated health check can monitor	255
Maximum total length of headers in the response to a health check request	16,384 bytes (16K)

Quotas on query log configurations

Entity	Quota
Query log configurations	1 per hosted zone

Quotas on traffic flow policies and policy records

Entity	Quota
Traffic policies	50 per AWS account
For more information about Route 53 traffic flow, see Using traffic flow to route DNS traffic (p. 442) .	Request a higher quota.
Traffic policy versions	1,000 per traffic policy
Traffic policy records (referred to as "policy instances" in the Route 53 API, AWS SDKs, AWS Command Line Interface, and AWS Tools for Windows PowerShell)	5 per AWS account Request a higher quota.

Quotas on reusable delegation sets

Entity	Quota
Reusable delegation sets	100 per AWS account Request a higher quota.

Maximums on API requests

Amazon Route 53 API requests are subject to the following maximums.

Topics

- [Number of elements and characters in ChangeResourceRecordSets requests \(p. 676\)](#)
- [Frequency of Amazon Route 53 API requests \(p. 676\)](#)
- [Frequency of Route 53 Resolver API requests \(p. 676\)](#)

Number of elements and characters in ChangeResourceRecordSets requests

ResourceRecord elements

A request cannot contain more than 1,000 ResourceRecord elements (including alias records). When the value of the Action element is UPSERT, each ResourceRecord element is counted twice.

Maximum number of characters

The sum of the number of characters (including spaces) in all Value elements in a request cannot exceed 32,000 characters. When the value of the Action element is UPSERT, each character in a Value element is counted twice.

Frequency of Amazon Route 53 API requests

All Amazon Route 53 API requests

For the [Amazon Route 53 APIs](#) five requests per second per AWS account. If you submit more than five requests per second, Amazon Route 53 returns an HTTP 400 error (Bad request). The response header also includes a Code element with a value of Throttling and a Message element with a value of Rate exceeded.

Note

If your application exceeds this limit, we recommend that you implement exponential backoff for retries. For more information, see [Error Retries and Exponential Backoff in AWS](#) in the *Amazon Web Services General Reference*.

ChangeResourceRecordSets requests

If Route 53 can't process a request before the next request arrives, it will reject subsequent requests for the same hosted zone and return an HTTP 400 error (Bad request). The response header also includes a Code element with a value of PriorRequestNotComplete and a Message element with a value of The request was rejected because Route 53 was still processing a prior request.

CreateHealthCheck requests

You can submit a maximum of 1,000 CreateHealthCheck requests in a 24-hour period.

Frequency of Route 53 Resolver API requests

All requests

Five requests per second per AWS account per Region. If you submit more than five requests per second in a Region, Resolver returns an HTTP 400 error (Bad request). The response header also includes a Code element with a value of Throttling and a Message element with a value of Rate exceeded.

Note

If your application exceeds this limit, we recommend that you implement exponential backoff for retries. For more information, see [Error Retries and Exponential Backoff in AWS](#) in the *Amazon Web Services General Reference*.

Related information

The following related resources can help you as you work with this service.

Topics

- [AWS resources \(p. 678\)](#)
- [Third-party tools and libraries \(p. 679\)](#)
- [Graphical user interfaces \(p. 679\)](#)

AWS resources

Several helpful guides, forums, and other resources are available from Amazon Web Services.

- [Amazon Route 53 API Reference](#) – A reference guide that includes the schema location; complete descriptions of the API actions, parameters, and data types; and a list of errors that the service returns.
- [**AWS::Route53::RecordSet Type in the AWS CloudFormation User Guide**](#) – A property for using Amazon Route 53 with AWS CloudFormation to create customized DNS names for your AWS CloudFormation stacks.
- [Discussion Forums](#) – A community-based forum for developers to discuss technical questions related to Route 53.
- [AWS Support Center](#) – This site brings together information about your recent support cases and results from AWS Trusted Advisor and health checks, as well as providing links to discussion forums, technical FAQs, the service health dashboard, and information about AWS support plans.
- [AWS Premium Support Information](#) – The primary web page for information about AWS Premium Support, a one-on-one, fast-response support channel to help you build and run applications on AWS Infrastructure Services.
- [Contact Us](#) – Links for inquiring about your billing or account. For technical questions, use the discussion forums or support links above.
- [Route 53 product information](#) – The primary web page for information about Route 53, including features, pricing, and more.
- [Classes & Workshops](#) – Links to role-based and specialty courses, in addition to self-paced labs to help sharpen your AWS skills and gain practical experience.
- [AWS Developer Tools](#) – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- [AWS Whitepapers](#) – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- [AWS Support Center](#) – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- [AWS Support](#) – The primary webpage for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- [Contact Us](#) – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- [AWS Site Terms](#) – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.

Third-party tools and libraries

In addition to AWS resources, you can find a variety of third-party tools and libraries that work with Amazon Route 53.

- [AmazonRoute53AppsScript \(via webos-goodies\)](#)

Google spreadsheet management of Amazon Route 53.

- [AWS Component for .NET \(via SprightlySoft\)](#)

SprightlySoft .NET Component for Amazon Web Services with support for REST operations and Route 53.

- [Boto API download \(via github\)](#)

Boto Python interface to Amazon Web Services.

- [cli53 \(via github\)](#)

Command line interface for Route 53.

- [Dasein Cloud API](#)

Java-based API.

- [R53.py \(via github\)](#)

Maintains a canonical version of your DNS configurations under source control, and calculates the minimum set of changes that are required to change a configuration.

- [RightScripts \(via RightScale\)](#)

Scripts to configure or update your RightScale server for use with Route 53.

- [RightScale Support Tutorials](#)

RightScale tutorial for domain setup with Route 53.

- [route53d](#)

DNS front-end to Route 53 API (enables incremental zone transfer (IXFR)).

- [Route53Manager \(via github\)](#)

Web-based interface.

- [Ruby Fog \(via github\)](#)

The Ruby cloud services library.

- [Valet \(via github\)](#)

Java API, including a one-way-sync utility for Windows DNS server files.

- [WebService::Amazon::Route53 \(via CPAN\)](#)

Perl interface to Amazon Route 53 API.

Graphical user interfaces

The following third-party tools provide graphical user interfaces (GUIs) for working with Amazon Route 53:

- [R53 Fox](#)

- [Ylastic](#)

Document history

The following entries describe important changes in each release of the Route 53 documentation. For notification about updates to this documentation, you can subscribe to an RSS feed.

Topics

- [2022 releases \(p. 681\)](#)
- [2021 releases \(p. 681\)](#)
- [2020 releases \(p. 682\)](#)
- [2018 releases \(p. 682\)](#)
- [2017 releases \(p. 683\)](#)
- [2016 releases \(p. 684\)](#)
- [2015 releases \(p. 686\)](#)
- [2014 releases \(p. 688\)](#)
- [2013 releases \(p. 690\)](#)
- [2012 release \(p. 691\)](#)
- [2011 releases \(p. 691\)](#)
- [2010 release \(p. 691\)](#)

2022 releases

March 16, 2022

Geolocation and latency-based routing options are now supported for private hosted zones in Amazon Route 53. For more information, see [Supported routing policies for records in a private hosted zone \(p. 357\)](#).

January 25, 2022

The process for changing ownership for .com.au and .net.au TLDs has been simplified to include responding to two emails (by both old and new registrants) and doesn't include filling in forms. For more information, see [.com.au \(Australia\) \(p. 295\)](#) and [.net.au \(Australia\) \(p. 301\)](#).

2021 releases

October 26, 2021

Added support for disabling default reverse DNS rules with Amazon Route 53. You can now disable the creation of these rules and instead forward queries for reverse DNS namespaces to external servers if desired. For more information, see [Forwarding rules for reverse DNS queries in Resolver \(p. 495\)](#).

September 1, 2021

Added a new getting started topic that walks you through creating Amazon CloudFront distributions for a static website. For more information, see [Use an Amazon CloudFront distribution to serve a static website \(p. 26\)](#).

July 14, 2021

Started tracking AWS managed policies for Amazon Route 53. For more information, see [AWS managed policies for Amazon Route 53 \(p. 590\)](#).

March 31, 2021

Added Route 53 Resolver DNS Firewall. With DNS Firewall you can provide protection for outbound DNS requests from your VPCs. For more information, see [Route 53 Resolver DNS Firewall \(p. 554\)](#).

2020 releases

December 17, 2020

Added support for DNSSEC signing for Route 53 Resolver. For more information, see [Configuring DNSSEC signing in Amazon Route 53 \(p. 455\)](#).

Added support for DNSSEC validation for Route 53 Resolver. For more information, see [Enabling DNSSEC validation in Amazon Route 53 \(p. 495\)](#).

September 23, 2020

Updated the entire Route 53 guide with the new console experience. For more information, see [What is Amazon Route 53? \(p. 1\)](#).

September 1, 2020

Added support for Resolver query logs. For more information, see [Resolver query logging \(p. 619\)](#).

2018 releases

December 20, 2018

You can create Route 53 alias records that route traffic to API Gateway APIs or to Amazon VPC interface endpoints. For more information, see [Value/route traffic to \(p. 404\)](#).

November 28, 2018

Route 53 Auto Naming (also known as Service Discovery) is now a separate service, AWS Cloud Map. For more information, see the [AWS Cloud Map Developer Guide](#).

November 19, 2018

You can use Route 53 Resolver to configure DNS resolution between your VPC and your network over a Direct Connect or VPN connection. (Resolver is the new name for the recursive DNS service that is provided to all customers by default in Amazon Virtual Private Cloud (Amazon VPC).) This lets you forward DNS queries from resolvers on your network to Route 53 Resolver. Resolver also lets you forward queries for selected domain names (example.com) and subdomain names (api.example.com) from a VPC to resolvers on your network. For more information, see [Resolving DNS queries between VPCs and your network \(p. 471\)](#).

November 7, 2018

When you're using Route 53 traffic flow and geoproximity routing, you can use an interactive map to visualize how your end users will be routed to your endpoints around the world. For more information, see [Viewing a map that shows the effect of geoproximity settings \(p. 448\)](#).

October 18, 2018

You can use the Route 53 console and API to temporarily disable a Route 53 health check. This gives you an easy way to pause monitoring of an endpoint, such as a web server, so that you can perform maintenance on it without triggering alarms or generating unnecessary logs or status messages.

For more information, see "Disabled" in [Values that you specify when you create or update health checks \(p. 519\)](#). The feature is available for all three types of Route 53 health checks: health checks that monitor an endpoint, health checks that monitor other health checks, and health checks that monitor a CloudWatch alarm.

March 13, 2018

If you're using auto naming, you can now use a third-party health checker to evaluate the health of your resources. This is useful when a resource isn't available over the internet, for example, because the instance is in an Amazon VPC. For more information, see [HealthCheckCustomConfig](#) in the [Amazon Route 53 API Reference](#).

March 9, 2018

IAM now includes managed policies for auto naming. For more information, see [AWS managed policies for Amazon Route 53 \(p. 590\)](#).

February 6, 2018

You can now configure auto naming to create alias records that route traffic to ELB load balancers or to create CNAME records. For more information, see [Attributes](#) in the documentation for the [RegisterInstance](#) API in the [Amazon Route 53 API Reference](#).

2017 releases

December 5, 2017

You can now use the Route 53 autonaming API to provision instances for microservices. Autonaming lets you automatically create DNS records and, optionally, health checks based on a template that you define. For more information, see [What is AWS Cloud Map?](#) in the [AWS Cloud Map Developer Guide](#).

November 16, 2017

You can now programmatically get both the current quotas on Route 53 resources such as hosted zones and health checks, and the number of each resource that you're currently using. For more information, see [GetAccountLimit](#), [GetHostedZoneLimit](#), and [GetReusableDelegationSetLimit](#) in the [Amazon Route 53 API Reference](#).

October 3, 2017

Route 53 is now a HIPAA eligible service. For more information, see [Compliance validation for Amazon Route 53 \(p. 613\)](#).

September 29, 2017

You can now programmatically check whether a domain can be transferred to Route 53. For more information, see [CheckDomainTransferability](#) in the [Amazon Route 53 API Reference](#).

September 11, 2017

You can now create Route 53 alias records that route internet traffic to Elastic Load Balancing Network Load Balancers. For more information about alias records, see [Choosing between alias and non-alias records \(p. 379\)](#).

September 7, 2017

If you're using Route 53 as your public, authoritative DNS service, you can now log DNS queries that Route 53 receives. For more information, see [Public DNS query logging \(p. 615\)](#).

September 1, 2017

If you're using Route 53 traffic flow, you can now use geoproximity routing, which lets you route traffic based on the physical distance between your users and your resources. You can also route

more or less traffic to each resource by specifying a positive or negative bias. For more information, see [Geoproximity routing \(traffic flow only\) \(p. 373\)](#).

August 21, 2017

You can now use Route 53 to create Certification Authority Authorization (CAA) records, which let you specify the certificate authorities that can issue certificates for your domains and subdomains. For more information, see [CAA record type \(p. 383\)](#).

August 18, 2017

You can now transfer large numbers of domains to Route 53 using the Route 53 console. For more information, see [Transferring registration for a domain to Amazon Route 53 \(p. 67\)](#).

August 4, 2017

When you register a domain, the registries for some top-level domains (TLDs) require you to verify that you specified a valid email address for the registrant contact. You can now send the verification email and get confirmation that you successfully verified the email address during the domain registration process. For more information, see [Registering a new domain \(p. 42\)](#).

June 21, 2017

If you want to route traffic approximately randomly to multiple resources, such as web servers, you can now create one multivalue answer record for each resource and, optionally, associate a Route 53 health check with each record. Route 53 responds to DNS queries with up to eight healthy records in response to each DNS query, and gives different answers to different DNS resolvers. For more information, see [Multivalue answer routing \(p. 378\)](#).

April 10, 2017

When you use the Route 53 console to transfer a domain registration to Route 53, you can now choose one of the following options for associating the name servers for the DNS service for the domain with the transferred domain registration:

- Use the name servers for a Route 53 hosted zone that you choose
- Use the name servers for the current DNS service for the domain
- Use name servers that you specify

Route 53 automatically associates these name servers with the transferred domain registration.

2016 releases

November 21, 2016

You can now create health checks that use IPv6 addresses to check the health of endpoints. For more information, see [Creating and updating health checks \(p. 519\)](#).

November 15, 2016

You can now use a Route 53 API action to associate an Amazon VPC that you created with one account with a private hosted zone that you created with another account. For more information, see [Associating an Amazon VPC and a private hosted zone that you created with different AWS accounts \(p. 361\)](#).

August 30, 2016

With this release, Route 53 adds the following new features:

- **Name Authority Pointer (NAPTR) records** – You can now create NAPTR records, which are used by Dynamic Delegation Discovery System (DDDS) applications to convert one value to another or to

replace one value with another. For example, one common use is to convert phone numbers into SIP URIs. For more information, see [NAPTR record type \(p. 387\)](#).

- **DNS query test tool** – You can now simulate DNS queries for a record and see the value that Route 53 returns. For geolocation and latency records, you can also simulate requests from a particular DNS resolver and/or client IP address to find out what response Route 53 would return to a client with that resolver and/or IP address. For more information, see [Checking DNS responses from Route 53 \(p. 347\)](#).

August 11, 2016

With this release, you can create alias records that route traffic to ELB Application Load Balancers. The process is the same as for Classic Load Balancers. For more information, see [Value/route traffic to \(p. 404\)](#).

August 9, 2016

With this release, Route 53 adds support for DNSSEC for domain registration. DNSSEC lets you protect your domain from DNS spoofing attacks, which are also known as man-in-the-middle attacks. For more information, see [Configuring DNSSEC for a domain \(p. 89\)](#).

July 7, 2016

You can now manually extend the registration for a domain and register a domain with an initial registration period longer than the minimum registration period specified by the registry. For more information, see [Extending the registration period for a domain \(p. 59\)](#).

July 6, 2016

If you're an AISPL customer with a contact address in India, you can now use Route 53 to register domains. For more information, see [Managing an Account in India](#).

May 26, 2016

With this release, Route 53 adds the following new features:

- **Domain billing report** – You can now download a report that lists all domain registration charges, by domain, for a specified time period. The report includes all domain registration operations for which there is a fee, including registering domains, transferring domains to Route 53, renewing domain registration, and (for some TLDs), changing the owner of a domain. For more information, see the following documentation:
 - [Route 53 console](#) – See [Downloading a domain billing report \(p. 96\)](#)
 - [Route 53 API](#) – See [ViewBilling](#) in the [Amazon Route 53 API Reference](#).
- **New TLDs** – You can now register domains that have the following TLDs: .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website, and .uk. For more information, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).
- **New APIs for domain registration** – For operations that require confirmation that the email address for the registrant contact is valid, such as registering a new domain, you can now programmatically determine whether the registrant contact has clicked the link in the confirmation email and, if not, whether the link is still valid. You can also programmatically request that we send another confirmation email. For more information, see the following documentation in the [Amazon Route 53 API Reference](#):
 - [GetContactReachabilityStatus](#)
 - [ResendContactReachabilityEmail](#)

April 5, 2016

With this release, Route 53 adds the following new features:

- **Health checks based on CloudWatch metrics** – You can now create health checks that are based on the alarm state of any CloudWatch metric. This is useful for checking the health of endpoints that can't be reached by a standard Route 53 health check, such as instances within an Amazon Virtual Private Cloud (VPC) that have only private IP addresses. For more information, see the following documentation:

- **Route 53 console** – See [Monitoring a CloudWatch alarm \(p. 523\)](#) in the "Values that You Specify When You Create or Update Health Checks" topic.
- **Route 53 API** – See [CreateHealthCheck](#) and [UpdateHealthCheck](#) in the *Amazon Route 53 API Reference*.
- **Configurable health check locations** – You can now choose the Route 53 health checking regions that check the health of your resources, which reduces the load on the endpoint from health checks. This is useful if your customers are concentrated in one or a few geographic regions. For more information, see the following documentation:
 - **Route 53 console** – See [Health checker regions](#) in the "Values that You Specify When You Create or Update Health Checks" topic.
 - **Route 53 API** – See the `Regions` element for [CreateHealthCheck](#) and [UpdateHealthCheck](#) in the *Amazon Route 53 API Reference*.
- **Failover in private hosted zones** – You can now create failover and failover alias records in a private hosted zone. When you combine this feature with metric-based health checks, you can configure DNS failover even for endpoints that have only private IP addresses and can't be reached by using standard Route 53 health checks. For more information, see the following documentation:
 - **Route 53 console** – See [Configuring failover in a private hosted zone \(p. 550\)](#).
 - **Route 53 API** – See [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.
- **Alias records in private hosted zones** – In the past, you could create alias records that route DNS queries only to other Route 53 records in the same hosted zone. With this release, you can also create alias records that route DNS queries to Elastic Beanstalk environments that have regionalized subdomains, Elastic Load Balancing load balancers, and Amazon S3 buckets. (You still can't create alias records that route DNS queries to a CloudFront distribution.) For more information, see the following documentation:
 - **Route 53 console** – See [Choosing between alias and non-alias records \(p. 379\)](#).
 - **Route 53 API** – See [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

February 23, 2016

When you create or update HTTPS health checks, you can now configure Route 53 to send the host name to the endpoint during TLS negotiation. This allows the endpoint to respond to the HTTPS request with the applicable SSL/TLS certificate. For more information, see the description for the `Enable SNI` field in the "Values that You Specify When You Create or Update Health Checks" topic. For information about how to enable SNI when you use the API to create or update a health check, see [CreateHealthCheck](#) and [UpdateHealthCheck](#) in the *Amazon Route 53 API Reference*.

January 27, 2016

You can now register domains for over 100 additional top-level domains (TLDs) such as .accountants, .band, and .city. For a complete list of supported TLDs, see [Domains that you can register with Amazon Route 53 \(p. 97\)](#).

January 19, 2016

You can now create alias records that route traffic to Elastic Beanstalk environments. For information about creating records by using the Route 53 console, see [Creating records by using the Amazon Route 53 console \(p. 392\)](#). For information about using the API to create records, see [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

2015 releases

December 3, 2015

The Route 53 console now includes a visual editor that lets you quickly create complex routing configurations that use a combination of Route 53 weighted, latency, failover, and geolocation

routing policies. You can then associate the configuration with one or more domain names (such as example.com) or subdomain names (such as www.example.com), in the same hosted zone or in multiple hosted zones. In addition, you can roll back the updates if the new configuration isn't performing as you expected it to. The same functionality is available by using the Route 53 API, AWS SDKs, the AWS CLI, and AWS Tools for Windows PowerShell. For information about using the visual editor, see [Using traffic flow to route DNS traffic \(p. 442\)](#). For information about using the API to create traffic flow configurations, see the [Amazon Route 53 API Reference](#).

October 19, 2015

With this release, Route 53 adds the following new features:

- **Domain registration for .com and .net domains by Amazon Registrar, Inc.** – Amazon is now an ICANN-accredited registrar for the .com and .net top-level domains (TLDs) through Amazon Registrar, Inc. When you use Route 53 to register a .com or .net domain, Amazon Registrar will be the registrar of record and will be listed as the "Sponsoring Registrar" in your Whois query results. For information about using Route 53 to register domains, see [Registering domain names using Amazon Route 53 \(p. 41\)](#).
- **Privacy protection for .com and .net domains** – When you register a .com or .net domain with Route 53, all of your personal information, including first and last name, is now hidden. First and last name are not hidden for other domains that you register with Route 53. For more information about privacy protection, see [Enabling or disabling privacy protection for contact information for a domain \(p. 57\)](#).

September 15, 2015

With this release, Route 53 adds the following new features:

- **Calculated health checks** – You can now create health checks whose status is determined by the health status of other health checks. For more information, see [Creating and updating health checks \(p. 519\)](#). In addition, see [CreateHealthCheck](#) in the [Amazon Route 53 API Reference](#).
- **Latency measurements for health checks** – You can now configure Route 53 to measure the latency between health checkers and your endpoint. Latency data appears in Amazon CloudWatch graphs in the Route 53 console. To enable latency measurements for new health checks, see the **Latency measurements** setting under [Advanced configuration \("Monitor an Endpoint" only\) \(p. 525\)](#) in the topic [Values that you specify when you create or update health checks \(p. 519\)](#). (You can't enable latency measurements for existing health checks.) In addition, see [MeasureLatency](#) in the topic [CreateHealthCheck](#) in the [Amazon Route 53 API Reference](#).
- **Updates to the health checks dashboard in the Route 53 console** – The dashboard for monitoring health checks has been improved in a variety of ways, including CloudWatch graphs for monitoring latency between Route 53 health checkers and your endpoints. For more information, see [Monitoring health check status and getting notifications \(p. 530\)](#).

March 3, 2015

The *Amazon Route 53 Developer Guide* now explains how to configure white-label name servers for Route 53 hosted zones. For more information, see [Configuring white-label name servers \(p. 349\)](#).

February 26, 2015

You can now use the Route 53 API to list the hosted zones that are associated with an AWS account in alphabetical order by name. You can also get a count of the hosted zones that are associated with an account. For more information, see [ListHostedZonesByName](#) and [GetHostedZoneCount](#) in the [Amazon Route 53 API Reference](#).

February 11, 2015

With this release, Route 53 adds the following new features:

- **Health Check Status** – The health checks page in the Route 53 console now includes a **Status** column that lets you view the overall status of all of your health checks. For more information, see [Viewing health check status and the reason for health check failures \(p. 530\)](#).

- **Integration with AWS CloudTrail** – Route 53 now works with CloudTrail to capture information about every request that your AWS account (including your IAM users) sends to the Route 53 API. Integrating Route 53 and CloudTrail lets you determine which requests were made to the Route 53 API, the source IP address from which each request was made, who made the request, when it was made, and more. For more information, see [Logging Amazon Route 53 API calls with AWS CloudTrail \(p. 635\)](#).
- **Quick Alarms for Health Checks** – When you create a health check by using the Route 53 console, you can now simultaneously create an Amazon CloudWatch alarm for the health check and specify who to notify when Route 53 considers the endpoint unhealthy for one minute. For more information, see [Creating and updating health checks \(p. 519\)](#).
- **Tagging for Hosted Zones and Domains** – You can now assign tags, which are commonly used for cost allocation, to Route 53 hosted zones and domains. For more information, see [Tagging Amazon Route 53 resources \(p. 655\)](#).

February 5, 2015

You can now use the Route 53 console to update contact information for a domain. For more information, see [Values that you specify when you register or transfer a domain \(p. 47\)](#).

January 22, 2015

You can now specify internationalized domain names when you're registering a new domain name with Route 53. (Route 53 already supported internationalized domain names for hosted zones and records.) For more information, see [DNS domain name format \(p. 38\)](#).

2014 releases

November 25, 2014

With this release, you can now edit the comment that you specified for a hosted zone when you created it. In the console, you just click the pencil icon next to the **Comment** field and enter a new value. For more information about changing the comment by using the Route 53 API, see [UpdateHostedZoneComment in the Amazon Route 53 API Reference](#).

November 5, 2014

With this release, Route 53 adds the following new features:

- **Private DNS for VPCs created using the Amazon Virtual Private Cloud service** – You can now use Route 53 to manage your internal domain names for VPCs without exposing DNS data to the public internet. For more information, see [Working with private hosted zones \(p. 356\)](#).
- **Health check failure reasons** – You can now see the current status of a selected health check, as well as details on why the health check last failed, as reported by each of the Route 53 health checkers. The status includes the HTTP status code, and failure reasons include information about numerous types of failures, such as string matching failures and response timeouts. For more information, see [Viewing health check status and the reason for health check failures \(p. 530\)](#).
- **Reusable delegation sets** – You can now apply the same set of four authoritative name servers, known collectively as a delegation set, to multiple hosted zones that correspond with different domain names. This greatly simplifies the process of migrating DNS service to Route 53 and managing large numbers of hosted zones. Using reusable delegation sets currently requires that you use the Route 53 API or an AWS SDK. For more information, see the [Amazon Route 53 API Reference](#).
- **Improved geolocation routing** – We further improved the accuracy of geolocation routing by adding support for the edns-client-subnet extension of EDNS0. For more information, see [Geolocation routing \(p. 372\)](#).
- **Support for Signature v4** – You can now sign all Route 53 API requests using Signature version 4. For more information, see [Signing Route 53 API Requests in the Amazon Route 53 API Reference](#).

July 31, 2014

With this release, you can now do the following:

- Register domain names using Route 53. For more information, see [Registering domain names using Amazon Route 53 \(p. 41\)](#).
- Configure Route 53 to respond to DNS queries based on the geographic location that the queries originate from. For more information, see [Geolocation routing \(p. 372\)](#).

July 2, 2014

With this release, you can now do the following:

- Edit most values in health checks. For more information, see [Creating, updating, and deleting health checks \(p. 518\)](#).
- Use the Route 53 API to get a list of the IP ranges that Route 53 health checkers use to check the health of your resources. You can use these IP addresses to configure your router and firewall rules to allow health checkers to check the health of your resources. For more information, see [GetCheckerIpRanges](#) in the *Amazon Route 53 API Reference*.
- Assign cost allocation tags to health checks, which also lets you assign a name to health checks. For more information, see [Naming and tagging health checks \(p. 551\)](#).
- Use the Route 53 API to get the number of health checks that are associated with your AWS account. For more information, see [GetHealthCheckCount](#) in the *Amazon Route 53 API Reference*.

April 30, 2014

With this release, you can now create health checks and use a domain name instead of an IP address to specify the endpoint. This is helpful when an endpoint's IP address either is not fixed or is served by multiple IPs, such as Amazon EC2 or Amazon RDS instances. For more information, see [Creating and updating health checks \(p. 519\)](#).

In addition, some information about using the Route 53 API that formerly appeared in the *Amazon Route 53 Developer Guide* has been moved. Now all API documentation appears in the *Amazon Route 53 API Reference*.

April 18, 2014

With this release, Route 53 passes a different value in the **Host** header when the health check **Port** value is **443** and the **Protocol** value is **HTTPS**. During a health check, Route 53 now passes to the endpoint a **Host** header that contains the value of the **Host Name** field. If you created the health check by using the `CreateHealthCheck` API action, this is the value of the `FullyQualifiedDomainName` element.

For more information, see [Creating, updating, and deleting health checks \(p. 518\)](#).

April 9, 2014

With this release, you can now view what percentage of Route 53 health checkers are currently reporting that an endpoint is healthy.

In addition, behavior of the Health Check Status metric in Amazon CloudWatch now shows only zero (if your endpoint was unhealthy during a given time period) or one (if the endpoint was healthy for that time period). The metric no longer shows values between 0 and 1 reflecting the portion of Route 53 health checks that are reporting the endpoint as healthy.

For more information, see [Monitoring health checks using CloudWatch \(p. 532\)](#).

February 18, 2014

With this release, Route 53 adds the following features:

- **Health check failover threshold:** You can now specify how many consecutive health checks an endpoint must fail before Route 53 considers the endpoint unhealthy, between 1 and 10 consecutive checks. An unhealthy endpoint must pass the same number of checks to be

considered healthy. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

- **Health check request interval:** You can now specify how frequently Route 53 sends requests to an endpoint to determine whether the endpoint is healthy. Valid settings are 10 seconds and 30 seconds. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

January 30, 2014

With this release, Route 53 adds the following features:

- **HTTP and HTTPS string-match health checks:** Route 53 now supports health checks that determine the health of an endpoint based on the appearance of a specified string in the response body. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).
- **HTTPS health checks:** Route 53 now supports health checks for secure, SSL-only websites. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).
- **UPSERT for the ChangeResourceRecordSets API Action:** When creating or changing records using the ChangeResourceRecordSets API action, you can now use the UPSERT action either to create a new record if none exists with a given name and type, or to update an existing record. For more information, see [ChangeResourceRecordSets](#) in the *Amazon Route 53 API Reference*.

January 7, 2014

With this release, Route 53 adds support for health checks that determine the health of an endpoint based on whether a specified string appears in the response body. For more information, see [How Amazon Route 53 determines whether a health check is healthy \(p. 516\)](#).

2013 releases

August 14, 2013

With this release, Route 53 adds support for creating records by importing a BIND-formatted zone file. For more information, see [Creating records by importing a zone file \(p. 438\)](#).

In addition, CloudWatch metrics for Route 53 health checks have been integrated into the Route 53 console and streamlined. For more information, see [Monitoring health checks using CloudWatch \(p. 532\)](#).

June 26, 2013

With this release, Route 53 adds support for integrating health checks with CloudWatch metrics so you can do the following:

- Verify that a health check is properly configured.
- Review the health of a health check endpoint over a specified period of time.
- Configure CloudWatch to send an Amazon Simple Notification Service (Amazon SNS) alert when all Route 53 health checkers consider your specified endpoint to be unhealthy.

For more information, see [Monitoring health checks using CloudWatch \(p. 532\)](#).

June 11, 2013

With this release, Route 53 adds support for creating alias records that route DNS queries to alternate domain names for Amazon CloudFront distributions. You can use this feature both for alternate domain names at the zone apex (example.com) and alternate domain names for subdomains (www.example.com). For more information, see [Routing traffic to an Amazon CloudFront distribution by using your domain name \(p. 498\)](#).

May 30, 2013

With this release, Route 53 adds support for evaluating the health of ELB load balancers and the associated Amazon EC2 instances. For more information, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

March 28, 2013

The documentation about health checks and failover was rewritten to enhance usability. For more information, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

February 11, 2013

With this release, Route 53 adds support for failover and health checks. For more information, see [Creating Amazon Route 53 health checks and configuring DNS failover \(p. 515\)](#).

2012 release

March 21, 2012

With this release, Route 53 lets you create latency records. For more information, see [Latency-based routing \(p. 377\)](#).

2011 releases

December 21, 2011

With this release, the Route 53 console in the AWS Management Console lets you create an alias record by choosing an Elastic Load Balancer from a list instead of manually entering the hosted zone ID and the DNS name of the load balancer. New functionality is documented in the *Amazon Route 53 Developer Guide*.

November 16, 2011

With this release, you can use the Route 53 console in the AWS Management Console to create and delete hosted zones, and to create, change, and delete records. New functionality is documented throughout the *Amazon Route 53 Developer Guide*, as applicable.

October 18, 2011

The *Amazon Route 53 Getting Started Guide* was merged into the *Amazon Route 53 Developer Guide*, and the *Developer Guide* was reorganized to enhance usability.

May 24, 2011

This release of Amazon Route 53 introduces alias records, which allow you to create zone apex aliases; weighted records; a new API (2011-05-05); and a service-level agreement. In addition, after six months in beta, Route 53 is now generally available. For more information, see the [Amazon Route 53 product page](#) and [Choosing between alias and non-alias records \(p. 379\)](#) in the *Amazon Route 53 Developer Guide*.

2010 release

December 5, 2010

This is the first release of *Amazon Route 53 Developer Guide*.

AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.