

Amazon Route 53 FAQs - Amazon Web Services

[aws.amazon.com \(https://aws.amazon.com/route53/faqs/\)](https://aws.amazon.com/route53/faqs/)

Getting Started

Q. What is a Domain Name System (DNS) Service?

DNS is a globally distributed service that translates human readable names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other. The Internet's DNS system works much like a phone book by managing the mapping between names and numbers. For DNS, the names are domain names (`www.example.com`) that are easy for people to remember and the numbers are IP addresses (`192.0.2.1`) that specify the location of computers on the Internet. DNS servers translate requests for names into IP addresses, controlling which server an end user will reach when they type a domain name into their web browser. These requests are called "queries."

Q. What is Amazon Route 53?

Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like `example.com` into the numeric IP addresses, such as `192.0.2.1`, that computers use to connect to each other. You can combine your DNS with health-checking services to route traffic to healthy endpoints or to independently monitor and/or alarm on endpoints. You can also purchase and manage domain names such as `example.com` and automatically configure DNS settings for your domains. Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS.

Q. What can I do with Amazon Route 53?

With Amazon Route 53, you can create and manage your public DNS records. Like a phone book, Route 53 lets you manage the IP addresses listed for your domain names in the Internet's DNS phone book. Route 53 also answers requests to translate specific domain names like `example.com` into their corresponding IP addresses like `192.0.2.1`. You can use Route 53 to create DNS records for a new domain or transfer DNS records for an existing domain. The simple, standards-based REST API for Route 53 allows you to easily create, update and manage DNS records. Route 53 additionally offers health checks to monitor the health and performance of your application as well as your web servers and other resources. You can also register new domain names or transfer in existing domain names to be managed by Route 53.

Q. How do I get started with Amazon Route 53?

Amazon Route 53 has a simple web service interface that lets you get started in minutes. Your DNS records are organized into “hosted zones” that you configure with the AWS Management Console or Route 53’s API. To use Route 53, you simply:

- Subscribe to the service by clicking on the sign-up button on the service page.
- If you already have a domain name:
 - Use the AWS Management Console or the CreateHostedZone API to create a hosted zone that can store DNS records for your domain. Upon creating the hosted zone, you receive four Route 53 name servers across four different Top-Level Domains (TLDs) to help ensure a high level of availability.
 - Additionally, you can transfer your domain name to Route 53’s management via either the AWS Management Console or the API.
- If you don't already have a domain name:
 - Use the AWS Management Console or the API to register your new domain name.
 - Route 53 automatically creates a hosted zone that stores DNS records for your domain. You also receive four Route 53 name servers across four different Top-Level Domains (TLDs) to help ensure a high level of availability.
- Your hosted zone will be initially populated with a basic set of DNS records, including four virtual name servers that will answer queries for your domain. You can add, delete or change records in this set by using the AWS Management Console or by calling the ChangeResourceRecordSet API. A list of supported DNS records is available [here](#).
- If your domain name is not managed by Route 53, you will need to inform the registrar with whom you registered your domain name to update the name servers for your domain to the ones associated with your hosted zone. If your domain name is managed by Route 53 already, your domain name will be automatically associated with the name servers hosting your zone.

Q. How does Amazon Route 53 provide high availability and low latency?

Route 53 is built using AWS’s highly available and reliable infrastructure. The globally distributed nature of our DNS servers helps ensure a consistent ability to route your end users to your application by circumventing any internet or network related issues. Route 53 is designed to provide the level of dependability required by important applications. Using a global anycast network of DNS servers around the world, Route 53 is designed to automatically answer queries from the optimal location depending on network conditions. As a result, the service offers low query latency for your end users.

Q. What are the DNS server names for the Amazon Route 53 service?

To provide you with a highly available service, each Amazon Route 53 hosted zone is served by its own set of virtual DNS servers. The DNS server names for each hosted zone are thus assigned by the system when that hosted zone is created.

Q. What is the difference between a Domain and a Hosted Zone?

A domain is a general DNS concept. Domain names are easily recognizable names for numerically addressed Internet resources. For example, amazon.com is a domain. A hosted zone is an Amazon Route 53 concept. A hosted zone is analogous to a traditional DNS zone file; it represents a collection of records that can be managed together, belonging to a single parent domain name. All resource record sets within a hosted zone must have the hosted zone's domain name as a suffix. For example, the amazon.com hosted zone may contain records named www.amazon.com, and www.aws.amazon.com, but not a record named www.amazon.ca. You can use the Route 53 Management Console or API to create, inspect, modify, and delete hosted zones. You can also use the Management Console or API to register new domain names and transfer existing domain names into Route 53's management.

Q. What is the price of Amazon Route 53?

Amazon Route 53 charges are based on actual usage of the service for Hosted Zones, Queries, Health Checks, and Domain Names. For full details, see the Amazon Route 53 pricing page (<https://aws.amazon.com/route53/pricing/>).

You pay only for what you use. There are no minimum fees, no minimum usage commitments, and no overage charges. You can estimate your monthly bill using the AWS Simple Monthly Calculator (<https://calculator.s3.amazonaws.com/index.html>).

Q. What types of access controls can I set for the management of my Domains on Amazon Route 53?

You can control management access to your Amazon Route 53 hosted zone by using the AWS Identity and Access Management (IAM) service. AWS IAM allows you to control who in your organization can make changes to your DNS records by creating multiple users and managing the permissions for each of these users within your AWS Account. Learn more about AWS IAM here (<https://aws.amazon.com/iam/>).

Q. I have subscribed for Amazon Route 53 but when I try to use the service it says "The AWS Access Key ID needs a subscription for the service."

When you sign up for a new AWS service, it can take up to 24 hours in some cases to complete activation, during which time you cannot sign up for the service again. If you've been waiting longer than 24 hours without receiving an email confirming activation, this could indicate a problem with your account or the authorization of your payment details. Please contact AWS Customer Service (<https://aws.amazon.com/contact-us/>) for help.

Q. Does Amazon Route 53 offer a Service Level Agreement (SLA)?

Yes. The Amazon Route 53 SLA provides for a service credit if a customer's monthly uptime percentage is below our service commitment in any billing cycle. More information can be found here (<https://aws.amazon.com/route53/sla/>).

Q. When is my hosted zone charged?

Hosted zones are billed once when they are created and then on the first day of each month.

Q. Why do I see two charges for the same hosted zone in the same month?

Hosted zones have a grace period of 12 hours--if you delete a hosted zone within 12 hours after you create it, we don't charge you for the hosted zone. After the grace period ends, we immediately charge the standard monthly fee for a hosted zone. If you create a hosted zone on the last day of the month (for example, January 31st), the charge for January might appear on the February invoice, along with the charge for February.

Q. Does Amazon Route 53 provide query logging capability?

You can configure Amazon Route 53 to log information about the queries that Amazon Route 53 receives including date-time stamp, domain name, query type, location etc. When you configure query logging, Amazon Route 53 starts to send logs to CloudWatch Logs. You use CloudWatch Logs tools to access the query logs. For more information please see our documentation (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html>).

Domain Name Systems (DNS)

Q. Does Amazon Route 53 use an anycast network?

Yes. Anycast is a networking and routing technology that helps your end users' DNS queries get answered from the optimal Route 53 location given network conditions. As a result, your users get high availability and improved performance with Route 53.

Q. Is there a limit to the number of hosted zones I can manage using Amazon Route 53?

Each Amazon Route 53 account is limited to a maximum of 500 hosted zones and 10,000 resource record sets per hosted zone. Complete our request for a higher limit (<https://aws.amazon.com/route53-request/>) and we will respond to your request within two business days.

Q. How can I import a zone into Route 53?

Route 53 supports importing standard DNS zone files which can be exported from many DNS providers as well as standard DNS server software such as BIND. For newly-created hosted zones, as well as existing hosted zones that are empty except for the default NS and SOA records, you can paste your zone file directly into the Route 53 console, and Route 53 automatically creates the records in your hosted zone. To get started with zone file import, read our walkthrough in the Amazon Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/rrs-changes-import-console.html>).

Q. Can I create multiple hosted zones for the same domain name?

Yes. Creating multiple hosted zones allows you to verify your DNS setting in a “test” environment, and then replicate those settings on a “production” hosted zone. For example, hosted zone Z1234 might be your test version of example.com, hosted on name servers ns-1, ns-2, ns-3, and ns-4. Similarly, hosted zone Z5678 might be your production version of example.com, hosted on ns-5, ns-6, ns-7, and ns-8. Since each hosted zone has a virtual set of name servers associated with that zone, Route 53 will answer DNS queries for example.com differently depending on which name server you send the DNS query to.

Q. Does Amazon Route 53 also provide website hosting?

No. Amazon Route 53 is an authoritative DNS service and does not provide website hosting (<https://aws.amazon.com/websites/>). However, you can use Amazon Simple Storage Service (Amazon S3) to host a static website. To host a dynamic website or other web applications, you can use Amazon Elastic Compute Cloud (Amazon EC2), which provides flexibility, control, and significant cost savings over traditional web hosting (<https://aws.amazon.com/websites/>) solutions. Learn more about Amazon EC2 here (<https://aws.amazon.com/ec2/>). For both static and dynamic websites, you can provide low latency delivery to your global end users with Amazon CloudFront. Learn more about Amazon CloudFront here (<https://aws.amazon.com/cloudfront/>).

Q. Which DNS record types does Amazon Route 53 support?

Amazon Route 53 currently supports the following DNS record types:

- A (address record)
- AAAA (IPv6 address record)
- CNAME (canonical name record)
- CAA (certification authority authorization)
- MX (mail exchange record)
- NAPTR (name authority pointer record)
- NS (name server record)
- PTR (pointer record)
- SOA (start of authority record)
- SPF (sender policy framework)
- SRV (service locator)
- TXT (text record)
- Amazon Route 53 also offers alias records, which are an Amazon Route 53-specific extension to DNS. You can create alias records to route traffic to selected AWS resources, including Amazon Elastic Load Balancing load balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, API Gateways, VPC interface endpoints, and Amazon S3 buckets that are configured as websites. Alias records typically have a type of A or AAAA, but they work like a CNAME record. Using an alias record, you can map your record name (example.com) to the DNS name for an AWS resource (elb1234.elb.amazonaws.com). Resolvers see the A or AAAA record and the IP address of the AWS resource.

We anticipate adding additional record types in the future.

Q. Does Amazon Route 53 support wildcard entries? If so, what record types support them?

Yes. To make it even easier for you to configure DNS settings for your domain, Amazon Route 53 supports wildcard entries for all record types, except NS records. A wildcard entry is a record in a DNS zone that will match requests for any domain name based on the configuration you set. For example, a wildcard DNS record such as *.example.com will match queries for www.example.com and subdomain.example.com.

Q. What is the default TTL for the various record types and can I change these values?

The time for which a DNS resolver caches a response is set by a value called the time to live (TTL) associated with every record. Amazon Route 53 does not have a default TTL for any record type. You must always specify a TTL for each record so that caching DNS resolvers can cache your DNS records to the length of time specified through the TTL.

Q. Can I use 'Alias' records with my sub-domains?

Yes. You can also use Alias records to map your sub-domains (www.example.com, pictures.example.com, etc.) to your ELB load balancers, CloudFront distributions, or S3 website buckets.

Q. Are changes to resource record sets transactional?

Yes. A transactional change helps ensure that the change is consistent, reliable, and independent of other changes. Amazon Route 53 has been designed so that changes complete entirely on any individual DNS server, or not at all. This helps ensure your DNS queries are always answered consistently, which is important when making changes such as flipping between destination servers. When using the API, each call to ChangeResourceRecordSets returns an identifier that can be used to track the status of the change. Once the status is reported as INSYNC, your change has been performed on all of the Route 53 DNS servers.

Q. Can I associate multiple IP addresses with a single record?

Yes. Associating multiple IP addresses with a single record is often used for balancing the load of geographically-distributed web servers. Amazon Route 53 allows you to list multiple IP addresses for an A record and responds to DNS requests with the list of all configured IP addresses.

Q. How quickly will changes I make to my DNS settings on Amazon Route 53 propagate globally?

Amazon Route 53 is designed to propagate updates you make to your DNS records to its world-wide network of authoritative DNS servers within 60 seconds under normal conditions. A change is successfully propagated world-wide when the API call returns an INSYNC status listing.

Note that caching DNS resolvers are outside the control of the Amazon Route 53 service and will cache your resource record sets according to their time to live (TTL). The INSYNC or PENDING status of a change refers only to the state of Route 53's authoritative DNS servers.

Q. Can I see a history of my changes and other operations on my Route 53 resources?

Yes, via AWS CloudTrail you can record and log the API call history for Route 53. Please reference the CloudTrail product page (<https://aws.amazon.com/cloudtrail/>) to get started.

Q. Can I use AWS CloudTrail logs to roll back changes to my hosted zones?

No. We recommend that you do not use CloudTrail logs to roll back changes to your hosted zones, because reconstruction of your zone change history using your CloudTrail logs may be incomplete.

Your AWS CloudTrail logs can be used for the purposes of security analysis, resource change tracking, and compliance auditing.

Q. Does Amazon Route 53 support DNSSEC?

Amazon Route 53 does not support DNSSEC for DNS at this time. But Amazon Route 53 allows DNSSEC on domain registration.

Q. Does Amazon Route 53 support IPv6?

Yes. Amazon Route 53 supports both forward (AAAA) and reverse (PTR) IPv6 records. The Amazon Route 53 service itself is also available over IPv6. Recursive DNS resolvers on IPv6 networks can use either IPv4 or IPv6 transport in order to submit DNS queries to Amazon Route 53. Amazon Route 53 health checks also support monitoring of endpoints using the IPv6 protocol.

Q. Can I point my zone apex (example.com versus www.example.com) at my Elastic Load Balancer?

Yes. Amazon Route 53 offers a special type of record called an 'Alias' record that lets you map your zone apex (example.com) DNS name to the DNS name for your ELB load balancer (such as my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com). IP addresses associated with load balancers can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one or more IP addresses for the load balancer. Route 53 supports alias records for three types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. There is no additional charge for queries to Alias records that are mapped to AWS ELB load balancers. These queries are listed as "Intra-AWS-DNS-Queries" on the Amazon Route 53 usage report.

Q. Can I point my zone apex (example.com versus www.example.com) at my website hosted on Amazon S3?

Yes. Amazon Route 53 offers a special type of record called an 'Alias' record that lets you map your zone apex (example.com) DNS name to your Amazon S3 website bucket (i.e. example.com.s3-website-us-west-2.amazonaws.com). IP addresses associated with Amazon S3 website endpoints can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one IP address for the bucket. Route 53 doesn't charge for queries to Alias records that are mapped to an S3 bucket that is

configured as a website. These queries are listed as “Intra-AWS-DNS-Queries” on the Amazon Route 53 usage report.

Q. Can I point my zone apex (example.com versus www.example.com) at my Amazon CloudFront distribution?

Yes. Amazon Route 53 offers a special type of record called an ‘Alias’ record that lets you map your zone apex (example.com) DNS name to your Amazon CloudFront distribution (for example, d123.cloudfront.net). IP addresses associated with Amazon CloudFront endpoints vary based on your end user’s location (in order to direct the end user to the nearest CloudFront edge location) and can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with the IP address(es) for the distribution. Route 53 doesn’t charge for queries to Alias records that are mapped to a CloudFront distribution. These queries are listed as “Intra-AWS-DNS-Queries” on the Amazon Route 53 usage report.

Q. Can I point my zone apex (example.com versus www.example.com) at my AWS Elastic Beanstalk environment?

Yes. Amazon Route 53 offers a special type of record called an ‘Alias’ record that lets you map your zone apex (example.com) DNS name to your AWS Elastic Beanstalk DNS name (i.e. example.elasticbeanstalk.com). IP addresses associated with AWS Elastic Beanstalk environments can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one or more IP addresses for the environment. Queries to Alias records that are mapped to AWS Elastic Beanstalk environments are free. These queries are listed as “Intra-AWS-DNS-Queries” on the Amazon Route 53 usage report.

Q. Can I point my zone apex (example.com versus www.example.com) at my Amazon API Gateway?

Yes. Amazon Route 53 offers a special type of record called an ‘Alias’ record that lets you map your zone apex (example.com) DNS name to your Amazon API Gateway DNS name (i.e. api-id.execute-api.region.amazonaws.com/stage). IP addresses associated with Amazon API Gateway can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one or more IP addresses for the API Gateway. There is no additional charge for queries to Alias records that are mapped to Amazon API Gateways. These queries are listed as “Intra-AWS-DNS-Queries” on the Route 53 usage report.

Q. Can I point my zone apex (example.com versus www.example.com) at my Amazon VPC endpoint?

Yes. Amazon Route 53 offers a special type of record called an ‘Alias’ record that lets you map your zone apex (example.com) DNS name to your Amazon VPC Endpoint DNS name (i.e. vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com). IP addresses associated with Amazon VPC Endpoints can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one or more IP addresses for the VPC endpoint. There is no additional charge for queries to Alias records that are mapped to Amazon VPC endpoints. These queries are listed as “Intra-AWS-DNS-Queries” on the Amazon Route 53 usage report.

Q. How can I use Amazon Route 53 with Amazon Simple Storage Service (Amazon S3) and Amazon CloudFront?

For websites delivered via Amazon CloudFront or static websites hosted on Amazon S3, you can use the Amazon Route 53 service to create an Alias record for your domain which points to the CloudFront distribution or S3 website bucket. For S3 buckets not configured to host static websites, you can create a CNAME record for your domain and the S3 bucket name. In all cases, note that you will also need to configure your S3 bucket or your CloudFront distribution respectively with the alternate domain name entry to completely establish the alias between your domain name and the AWS domain name for your bucket or distribution.

For CloudFront distributions and S3 buckets configured to host static websites, we recommend creating an 'Alias' record that maps to your CloudFront distribution or S3 website bucket, instead of using CNAMEs. Alias records have two advantages: first, unlike CNAMEs, you can create an Alias record for your zone apex (e.g. example.com, instead of www.example.com), and second, queries to Alias records are free of charge.

Q. Why does the DNS Query Test Tool return a response different than the dig or nslookup commands?

When resource record sets are changed in Amazon Route 53, the service propagates updates you make to your DNS records to its world-wide network of authoritative DNS servers. If you test the record before propagation is complete, you may see an old value when you use the dig or nslookup utilities. Additionally, DNS resolvers on the internet are outside the control of the Amazon Route 53 service and will cache your resource record sets according to their time to live (TTL), which means a dig/nslookup command might return a cached value. You should also make sure that your domain name registrar is using the name servers in your Amazon Route 53 hosted zone. If not, Amazon Route 53 will not be authoritative for queries to your domain.

DNS Routing Policies

Q. Does Amazon Route 53 support Weighted Round Robin (WRR)?

Yes. Weighted Round Robin allows you to assign weights to resource record sets in order to specify the frequency with which different responses are served. You may want to use this capability to do A/B testing, sending a small portion of traffic to a server on which you've made a software change. For instance, suppose you have two record sets associated with one DNS name—one with weight 3 and one with weight 1. In this case, 75% of the time Route 53 will return the record set with weight 3 and 25% of the time Route 53 will return the record set with weight 1. Weights can be any number between 0 and 255.

Q. What is Amazon Route 53's Latency Based Routing (LBR) feature?

LBR (Latency Based Routing) is a new feature for Amazon Route 53 that helps you improve your application's performance for a global audience. You can run applications in multiple AWS regions and Amazon Route 53, using dozens of edge locations worldwide, will route end users to the AWS region that provides the lowest latency.

Q. How do I get started using Amazon Route 53's Latency Based Routing (LBR) feature?

You can start using Amazon Route 53's new LBR feature quickly and easily by using either the AWS Management

Console or a simple API. You simply create a record set that includes the IP addresses or ELB names of various AWS endpoints and mark that record set as an LBR-enabled Record Set, much like you mark a record set as a Weighted Record Set. Amazon Route 53 takes care of the rest - determining the best endpoint for each request and routing end users accordingly, much like Amazon CloudFront, Amazon's global content delivery service, does. You can learn more about how to use Latency Based Routing in the Amazon Route 53 Developer Guide (<http://docs.amazonwebservices.com/Route53/latest/DeveloperGuide/CreatingLatencyRRSets.html>).

Q. What is the price for Amazon Route 53's Latency Based Routing (LBR) feature?

Like all AWS services, there are no upfront fees or long term commitments to use Amazon Route 53 and LBR. Customers simply pay for the hosted zones and queries they actually use. Please visit the Amazon Route 53 pricing page (<https://aws.amazon.com/route53/pricing/>) for details on pricing for Latency Based Routing queries.

Q. What is Amazon Route 53's Geo DNS feature?

Route 53 Geo DNS lets you balance load by directing requests to specific endpoints based on the geographic location from which the request originates. Geo DNS makes it possible to customize localized content, such as presenting detail pages in the right language or restricting distribution of content to only the markets you have licensed. Geo DNS also lets you balance load across endpoints in a predictable, easy-to-manage way, ensuring that each end-user location is consistently routed to the same endpoint. Geo DNS provides three levels of geographic granularity: continent, country, and state, and Geo DNS also provides a global record which is served in cases where an end user's location doesn't match any of the specific Geo DNS records you have created. You can also combine Geo DNS with other routing types, such as Latency Based Routing and DNS Failover, to enable a variety of low-latency and fault-tolerant architectures. For information on how to configure various routing types, please see the Amazon Route 53 documentation (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>).

Q. How do I get started using Amazon Route 53's Geo DNS feature?

You can start using Amazon Route 53's Geo DNS feature quickly and easily by using either the AWS Management Console or the Route 53 API. You simply create a record set and specify the applicable values for that type of record set, mark that record set as a Geo DNS-enabled Record Set, and select the geographic region (global, continent, country, or state) that you want the record to apply to. You can learn more about how to use Geo DNS in the Amazon Route 53 Developer Guide.

Q. When using Geo DNS, do I need a "global" record? When would Route 53 return this record?

Yes, we strongly recommend that you configure a global record, to ensure that Route 53 can provide a response to DNS queries from all possible locations—even if you have created specific records for each continent, country, or state where you expect your end users will be located. Route 53 will return the value contained in your global record in the following cases:

The DNS query comes from an IP address not recognized by Route 53's Geo IP database.

The DNS query comes from a location not included in any of the specific Geo DNS records you have created.

Q. Can I have a Geo DNS record for a continent and different Geo DNS records for countries within that continent? Or a Geo DNS record for a country and Geo DNS records for states within that country?

Yes, you can have Geo DNS records for overlapping geographic regions (e.g., a continent and countries within that continent, or a country and states within that country). For each end user's location, Route 53 will return the most specific Geo DNS record that includes that location. In other words, for a given end user's location, Route 53 will first return a state record; if no state record is found, Route 53 will return a country record; if no country record is found, Route 53 will return a continent record; and finally, if no continent record is found, Route 53 will return the global record.

Q. What is the price for Route 53's Geo DNS feature?

Like all AWS services, there are no upfront fees or long term commitments to use Amazon Route 53 and Geo DNS. Customers simply pay for the hosted zones and queries they actually use. Please visit the Amazon Route 53 pricing page (<https://aws.amazon.com/route53/pricing/>) for details on pricing for Geo DNS queries.

Q. What is the difference between Latency Based Routing and Geo DNS?

Geo DNS bases routing decisions on the geographic location of the requests. In some cases, geography is a good proxy for latency; but there are certainly situations where it is not. LatencyBased Routing utilizes latency measurements between viewer networks and AWS datacenters. These measurements are used to determine which endpoint to direct users toward.

If your goal is to minimize end-user latency, we recommend using Latency Based Routing. If you have compliance, localization requirements, or other use cases that require stable routing from a specific geography to a specific endpoint, we recommend using Geo DNS.

Q. Does Amazon Route 53 support multiple values in response to DNS queries?

Route 53 now supports multivalued answers in response to DNS queries. While not a substitute for a load balancer, the ability to return multiple health-checkable IP addresses in response to DNS queries is a way to use DNS to improve availability and load balancing. If you want to route traffic randomly to multiple resources, such as web servers, you can create one multivalued answer record for each resource and, optionally, associate an Amazon Route 53 health check with each record. Amazon Route 53 supports up to eight healthy records in response to each DNS query.

Traffic Flow

Q. What is Amazon Route 53 Traffic Flow?

Amazon Route 53 Traffic Flow is an easy-to-use and cost-effective global traffic management service. With Amazon Route 53 Traffic Flow, you can improve the performance and availability of your application for your end users by running multiple endpoints around the world, using Amazon Route 53 Traffic Flow to connect your users to the best endpoint based on latency, geography, and endpoint health. Amazon Route 53 Traffic Flow makes it easy for developers to create policies that route traffic based on the constraints they care most about, including latency, endpoint health, load, geoproximity and geography. Customers can customize these templates or build policies from scratch using a simple visual policy builder in the AWS Management Console.

Q. What is the difference between a traffic policy and a policy record?

A traffic policy is the set of rules that you define to route end users' requests to one of your application's endpoints. You can create a traffic policy using the visual policy builder in the Amazon Route 53 Traffic Flow section of the Amazon Route 53 console. You can also create traffic policies as JSON-formatted text files and upload these policies using the Route 53 API, the AWS CLI, or the various AWS SDKs.

By itself, a traffic policy doesn't affect how end users are routed to your application because it isn't yet associated with your application's DNS name (such as `www.example.com`). To start using Amazon Route 53 Traffic Flow to route traffic to your application using the traffic policy you've created, you create a policy record which associates the traffic policy with the appropriate DNS name within an Amazon Route 53 hosted zone that you own. For example, if you want to use a traffic policy that you've named `my-first-traffic-policy` to manage traffic for your application at `www.example.com`, you will create a policy record for `www.example.com` within your hosted zone `example.com` and choose `my-first-traffic-policy` as the traffic policy.

Policy records are visible in both the Amazon Route 53 Traffic Flow and Amazon Route 53 Hosted Zone sections of the Amazon Route 53 console.

Q. Can I use the same policy to manage routing for more than one DNS name?

Yes. You can reuse a policy to manage more than one DNS name in one of two ways. First, you can create additional policy records using the policy. Note that there is an additional charge for using this method because you are billed for each policy record that you create.

The second method is to create one policy record using the policy, and then for each additional DNS name that you want to manage using the policy, you create a standard CNAME record pointing at the DNS name of the policy record that you created. For example, if you create a policy record for `example.com`, you can then create DNS records for `www.example.com`, `blog.example.com`, and `www.example.net` with a CNAME value of `example.com` for each record. Note that this method is not possible for records at the zone apex, such as `example.net`, `example.org`, or `example.co.uk` (without `www` or another subdomain in front of the domain name). For records at the zone apex, you must create a policy record using your traffic policy.

Q. Can I create an Alias record pointing to a DNS name that is managed by a traffic policy?

Yes, it is possible to create an Alias record pointing to a DNS name that is being managed by a traffic policy.

Q. Is there a charge for traffic policies that don't have a policy record?

No. We only charge for policy records; there is no charge for creating the traffic policy itself.

Q. How am I billed for using Amazon Route 53 Traffic Flow?

You are billed per policy record. A policy record represents the application of a Traffic Flow policy to a specific DNS name (such as `www.example.com`) in order to use the traffic policy to manage how requests for that DNS name are answered. Billing is monthly and is prorated for partial months. There is no charge for traffic policies that are not associated with a DNS name via a policy record. For details on pricing, see the Amazon Route 53 pricing page (<https://aws.amazon.com/route53/pricing/>).

Q. What are the advanced query types supported in Amazon Route 53 Traffic Flow?

Traffic Flow supports all Amazon Route 53 DNS Routing policies including latency, endpoint health, multivalue; answers, weighted round robin, and geo. In addition to these, Traffic Flow also supports geoproximity based routing with traffic biasing.

Q. How does a traffic policy using geoproximity rule route DNS traffic?

When you create a traffic flow policy, you can specify either an AWS region (if you're using AWS resources) or the latitude and longitude for each endpoint. For example, suppose you have EC2 instances in the AWS US East (Ohio) region and in the US West (Oregon) region. When an user in Seattle visits your website, geoproximity routing will route the DNS query to the EC2 instances in the US West (Oregon) region because it's closer geographically. For more information please see the documentation on geoproximity routing (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geoproximity>).

Q. How does the geoproximity bias value of an endpoint affect DNS traffic routing to other endpoints?

Changing the geoproximity bias value on an endpoint either expands or shrinks the area from which Route 53 routes traffic to a resource. The geoproximity bias can't accurately predict the load factor, though, because a small shift in the size of geographic areas might include or exclude major metropolitan areas that generate large numbers of queries. For more information please refer to our documentation (<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geoproximity>).

Q. Can I use bias for other Traffic Flow rules?

As of today, bias can only be applied to geoproximity rules.

Private DNS

Q. What is Private DNS?

Private DNS is a Route 53 feature that lets you have authoritative DNS within your VPCs without exposing your DNS records (including the name of the resource and its IP address(es) to the Internet.

Q. Can I use Amazon Route 53 to manage my organization's private IP addresses?

Yes, you can manage private IP addresses within Virtual Private Clouds (VPCs) using Amazon Route 53's Private DNS feature. With Private DNS, you can create a private hosted zone, and Route 53 will only return these records when queried from within the VPC(s) that you have associated with your private hosted zone. For more details, see the Amazon Route 53 Documentation (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html>).

Q. How do I set up Private DNS?

You can set up Private DNS by creating a hosted zone in Route 53, selecting the option to make the hosted zone "private", and associating the hosted zone with one of your VPCs. After creating the hosted zone, you can associate it with additional VPCs. See the Amazon Route 53 Documentation (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html>) for full details on how to configure Private DNS.

Q. Do I need connectivity to the outside Internet in order to use Private DNS?

You can resolve internal DNS names from resources within your VPC that do not have Internet connectivity. However, to update the configuration for your Private DNS hosted zone, you need Internet connectivity to access the Route 53 API endpoint, which is outside of VPC.

Q. Can I still use Private DNS if I'm not using VPC?

No. Route 53 Private DNS uses VPC to manage visibility and provide DNS resolution for private DNS hosted zones. To take advantage of Route 53 Private DNS, you must configure a VPC and migrate your resources into it.

Q. Can I use the same private Route 53 hosted zone for multiple VPCs?

Yes, you can associate multiple VPCs with a single hosted zone.

Q. Can I associate VPCs and private hosted zones that I created under different AWS accounts?

Yes, you can associate VPCs belonging to different accounts with a single hosted zone. You can see more details here (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs-different-accounts.html>).

Q. Will Private DNS work across AWS regions?

Yes. DNS answers will be available within every VPC that you associate with the private hosted zone. Note that you will need to ensure that the VPCs in each region have connectivity with each other in order for resources in one region to be able to reach resources in another region. Route 53 Private DNS is supported today in the US East (Northern Virginia), US West (Northern California), US West (Oregon), Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), EU (Frankfurt), EU (Ireland), and South America (Sao Paulo) regions.

Q. Can I configure DNS Failover for Private DNS hosted zones?

Yes, it is possible to configure DNS Failover by associating health checks with resource record sets within a Private DNS hosted zone. If your endpoints are within a Virtual Private Cloud (VPC), you have several options to configure health checks against these endpoints. If the endpoints have public IP addresses, then you can create a standard health check against the public IP address of each endpoint. If your endpoints only have private IP addresses, then you cannot create standard health checks against these endpoints. However, you can create metric based health checks, which function like standard Amazon Route 53 health checks except that they use an existing Amazon CloudWatch metric as the source of endpoint health information instead of making requests against the endpoint from external locations.

Q. Can I use Private DNS to block domains and DNS names that I don't want to be reached from within my VPC?

Yes, you can block domains and specific DNS names by creating these names in one or more Private DNS hosted zones and pointing these names to your own server (or another location that you manage).

Health Checks & DNS Failover

Q. What is DNS Failover?

DNS Failover consists of two components: health checks and failover. Health checks are automated requests sent over the Internet to your application to verify that your application is reachable, available, and functional. You can configure the health checks to be similar to the typical requests made by your users, such as requesting a web page from a specific URL. With DNS failover, Route 53 only returns answers for resources that are healthy and reachable from the outside world, so that your end users are routed away from a failed or unhealthy part of your application.

Q. How do I get started with DNS Failover?

Visit the Amazon Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks.html>) for details on getting started. You can also configure DNS Failover from within the Route 53 Console.

Q. Does DNS Failover support Elastic Load Balancers (ELBs) as endpoints?

Yes, you can configure DNS Failover for Elastic Load Balancers (ELBs). To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route

53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB. For more details on using DNS Failover with ELB endpoints, please consult the Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>).

Q. Can I configure a backup site to be used only when a health check fails?

Yes, you can use DNS Failover to maintain a backup site (for example, a static site running on an Amazon S3 website bucket) and fail over to this site in the event that your primary site becomes unreachable.

Q. What DNS record types can I associate with Route 53 health checks?

You can associate any record type supported by Route 53 except SOA and NS records.

Q. Can I health check an endpoint if I don't know its IP address?

Yes. You can configure DNS Failover for Elastic Load Balancers and Amazon S3 website buckets via the Amazon Route 53 Console without needing to create a health check of your own. For these endpoint types, Route 53 automatically creates and manages health checks on your behalf which are used when you create an Alias record pointing to the ELB or S3 website bucket and enable the "Evaluate Target Health" parameter on the Alias record.

For all other endpoints, you can specify either the DNS name (e.g. www.example.com) or the IP address of the endpoint when you create a health check for that endpoint.

Q. One of my endpoints is outside AWS. Can I set up DNS Failover on this endpoint?

Yes. Just like you can create a Route 53 resource record that points to an address outside AWS, you can set up health checks for parts of your application running outside AWS, and you can fail over to any endpoint that you choose, regardless of location. For example, you may have a legacy application running in a datacenter outside AWS and a backup instance of that application running within AWS. You can set up health checks of your legacy application running outside AWS, and if the application fails the health checks, you can fail over automatically to the backup instance in AWS.

Q. If failover occurs and I have multiple healthy endpoints remaining, will Route 53 consider the load on my healthy endpoints when determining where to send traffic from the failed endpoint?

No, Route 53 does not make routing decisions based on the load or available traffic capacity of your endpoints. You will need to ensure that you have available capacity at your other endpoints, or the ability to scale at those endpoints, in order to handle the traffic that had been flowing to your failed endpoint.

Q. How many consecutive health check observations does an endpoint need to fail to be considered "failed"?

The default is a threshold of three health check observations: when an endpoint has failed three consecutive observations, Route 53 will consider it failed. However, Route 53 will continue to perform health check observations on the endpoint and will resume sending traffic to it once it passes three consecutive observations. You can change this threshold to any value between 1 and 10 observations. For more details, see the Amazon Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-creating-deleting.html>).

Q. When my failed endpoint becomes healthy again, how is the DNS failover reversed?

After a failed endpoint passes the number of consecutive health check observations that you specify when creating the health check (the default threshold is three observations), Route 53 will restore its DNS records automatically, and traffic to that endpoint will resume with no action required on your part.

Q. What is the interval between health check observations?

By default, health check observations are conducted at an interval of 30 seconds. You can optionally select a fast interval of 10 seconds between observations.

By checking three times more often, fast interval health checks enable Route 53 to confirm more quickly that an endpoint has failed, shortening the time required for DNS failover to redirect traffic in response to the endpoint's failure.

Fast interval health checks also generate three times the number of requests to your endpoint, which may be a consideration if your endpoint has a limited capacity to serve web traffic. Visit the Route 53 pricing page (<http://aws.amazon.com/route53/pricing/>) for details on pricing for fast interval health checks and other optional health check features. For more details, see the Amazon Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-creating-deleting.html>).

Q. How much load should I expect a health check to generate on my endpoint (for example, a web server)?

Each health check is conducted from multiple locations around the world. The number and set of locations is configurable; you can modify the number of locations from which each of your health checks is conducted using the Amazon Route 53 console or API. Each location checks the endpoint independently at the interval that you select: the default interval of 30 seconds, or an optional fast interval of 10 seconds. Based on the current default number of health checking locations, you should expect your endpoint to receive one request every 2-3 seconds on average for standard interval health checks and one or more requests per second for fast-interval health checks.

Q. Do Route 53 health checks follow HTTP redirects?

No. Route 53 health checks consider an HTTP 3xx code to be a successful response, so they don't follow the redirect. This may cause unexpected results for string-matching health checks. The health check searches for the specified string in the body of the redirect. Because the health check doesn't follow the redirect, it never sends a request to the location that the redirect points to and never gets a response from that location. For string matching

health checks, we recommend that you avoid pointing the health check at a location that returns an HTTP redirect.

Q. What is the sequence of events when failover happens?

In simplest terms, the following events will take place if a health check fails and failover occurs:

Route 53 conducts a health check of your application. In this example, your application fails three consecutive health checks, triggering the following events.

Route 53 disables the resource records for the failed endpoint and no longer serves these records. This is the failover step, which causes traffic to begin being routed to your healthy endpoint(s) instead of your failed endpoint.

Q. Do I need to adjust the TTL for my records in order to use DNS Failover?

The time for which a DNS resolver caches a response is set by a value called the time to live (TTL) associated with every record. We recommend a TTL of 60 seconds or less when using DNS Failover, to minimize the amount of time it takes for traffic to stop being routed to your failed endpoint. In order to configure DNS Failover for ELB and S3 Website endpoints, you need to use Alias records which have fixed TTL of 60 seconds; for these endpoint types, you do not need to adjust TTLs in order to use DNS Failover.

Q. What happens if all of my endpoints are unhealthy?

Route 53 can only fail over to an endpoint that is healthy. If there are no healthy endpoints remaining in a resource record set, Route 53 will behave as if all health checks are passing.

Q. Can I use DNS Failover without using Latency Based Routing (LBR)?

Yes. You can configure DNS Failover without using LBR. In particular, you can use DNS failover to configure a simple failover scenario where Route 53 monitors your primary website and fails over to a backup site in the event that your primary site is unavailable.

Q. Can I configure a health check on a site accessible only via HTTPS?

Yes. Route 53 supports health checks over HTTPS, HTTP or TCP.

Q. Do HTTPS health checks validate the endpoint's SSL certificate?

No, HTTPS health checks test whether it's possible to connect with the endpoint over SSL and whether the endpoint returns a valid HTTP response code. However, they do not validate the SSL certificate returned by the endpoint.

Q. Do HTTPS health checks support Server Name Indication (SNI)?

Yes, HTTPS health checks support SNI.

Q. How can I use health checks to verify that my web server is returning the correct content?

You can use Route 53 health checks to check for the presence of a designated string in a server response by selecting the "Enable String Matching" option. This option can be used to check a web server to verify that the HTML it serves contains an expected string. Or, you can create a dedicated status page and use it to check the health of the server from an internal or operational perspective. For more details, see the Amazon Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-creating-deleting.html>).

Q. How do I see the status of a health check that I've created?

You can view the current status of a health check, as well as details on why it has failed, in the Amazon Route 53 console and via the Route 53 API.

Additionally, each health check's results are published as Amazon CloudWatch metrics showing the endpoint's health and, optionally, the latency of the endpoint's response. You can view a graph of the Amazon CloudWatch metric in the health checks tab of the Amazon Route 53 console to see the current and historical status of the health check. You can also create Amazon CloudWatch alarms on the metric in order to send notifications if the status of the health check changes.

The Amazon CloudWatch metrics for all of your Amazon Route 53 health checks are also visible in the Amazon CloudWatch console. Each Amazon CloudWatch metric contains the Health Check ID (for example, 01beb6a3-e1c2-4a2b-a0b7-7031e9060a6a) which you can use to identify which health check the metric is tracking.

Q. How can I measure the performance of my application's endpoints using Amazon Route 53?

Amazon Route 53 health checks include an optional latency measurement feature which provides data on how long it takes your endpoint to respond to a request. When you enable the latency measurement feature, the Amazon Route 53 health check will generate additional Amazon CloudWatch metrics showing the time required for Amazon Route 53's health checkers to establish a connection and to begin receiving data. Amazon Route 53 provides a separate set of latency metrics for each AWS region where Amazon Route 53 health checks are conducted.

Q. How can I be notified if one of my endpoints starts failing its health check?

Because each Route 53 health check publishes its results as a CloudWatch metric, you can configure the full range of CloudWatch notifications and automated actions which can be triggered when the health check value changes beyond a threshold that you specify. First, in either the Route 53 or CloudWatch console, configure a CloudWatch alarm on the health check metric. Then add a notification action and specify the email or SNS topic that you want to publish your notification to. Please consult the Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/monitoring-health-checks.html>) for full details.

Q: I created an alarm for my health check, but I need to re-send the confirmation email for the alarm's SNS topic.

How can I re-send this email?

Confirmation emails can be re-sent from the SNS console. To find the name of the SNS topic associated with the alarm, click the alarm name within the Route 53 console and looking in the box labeled "Send notification to."

Within the SNS console, expand the list of topics, and select the topic from your alarm. Open the "Create Subscription" box and select Email for protocol and enter the desired email address. Clicking "Subscribe" will re-send the confirmation email.

Q. I'm using DNS Failover with Elastic Load Balancers (ELBs) as endpoints. How can I see the status of these endpoints?

The recommended method for setting up DNS Failover with ELB endpoints is to use Alias records with the "Evaluate Target Health" option. Because you don't create your own health checks for ELB endpoints when using this option, there are no specific CloudWatch metrics generated by Route 53 for these endpoints.

You can get metrics on the health of your load balancer in two ways. First, Elastic Load Balancing publishes metrics that indicate the health of the load balancer and the number of healthy instances behind it. For details on configuring CloudWatch metrics for ELB, consult the ELB developer guide (http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/US_MonitoringLoadBalancerWithCW.html). Second, you can create your own health check against the CNAME provided by the ELB, e.g. `elb-example-123456678.us-west-2.elb.amazonaws.com`. You won't use this health check for DNS Failover itself (because the "Evaluate Target Health" option provides DNS Failover for you), but you can view the CloudWatch metrics for this health check and create alarms to be notified if the health check fails.

For complete details on using DNS Failover with ELB endpoints, please consult the Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>).

Q. For Alias records pointing to Amazon S3 Website buckets, what is being health checked when I set Evaluate Target Health to "true"?

Amazon Route 53 performs health checks of the Amazon S3 service itself in each AWS region. When you enable Evaluate Target Health on an Alias record pointing to an Amazon S3 Website bucket, Amazon Route 53 will take into account the health of the Amazon S3 service in the AWS region where your bucket is located. Amazon Route 53 does not check whether a specific bucket exists or contains valid website content; Amazon Route 53 will only fail over to another location if the Amazon S3 service itself is unavailable in the AWS region where your bucket is located.

Q. What is the cost to use CloudWatch metrics for my Route 53 health checks?

CloudWatch metrics for Route 53 health checks are available free of charge.

Q. Can I configure DNS Failover based on internal health metrics, such as CPU load, network, or memory?

Yes. Amazon Route 53's metric based health checks let you perform DNS failover based on any metric that is available within Amazon CloudWatch, including AWS-provided metrics and custom metrics from your own application. When you create a metric based health check within Amazon Route 53, the health check becomes unhealthy whenever its associated Amazon CloudWatch metric enters an alarm state.

Metric based health checks are useful to enable DNS failover for endpoints that cannot be reached by a standard Amazon Route 53 health check, such as instances within a Virtual Private Cloud (VPC) that only have private IP addresses. Using Amazon Route 53's calculated health check feature, you can also accomplish more sophisticated failover scenarios by combining the results of metric based health checks with the results of standard Amazon Route 53 health checks, which make requests against an endpoint from a network of checkers around the world. For example, you can create a configuration which fails away from an endpoint if either its public-facing web page is unavailable, or if internal metrics such as CPU load, network in/out, or disk reads show that the server itself is unhealthy.

Q. My web server is receiving requests from a Route 53 health check that I did not create. How can I stop these requests?

Occasionally, Amazon Route 53 customers create health checks that specify an IP address or domain name that does not belong to them. If your web server is getting unwanted HTTP(s) requests that you have traced to Amazon Route 53 health checks, please provide information on the unwanted health check using this form (<https://aws.amazon.com/forms/route53-unwanted-healthchecks>), and we will work with our customer to fix the problem.

Q. If I specify a domain name as my health check target, will Amazon Route 53 check over IPv4 or IPv6?

If you specify a domain name as the endpoint of an Amazon Route 53 health check, Amazon Route 53 will look up the IPv4 address of that domain name and will connect to the endpoint using IPv4. Amazon Route 53 will not attempt to look up the IPv6 address for an endpoint that is specified by domain name. If you want to perform a health check over IPv6 instead of IPv4, select "IP address" instead of "domain name" as your endpoint type, and enter the IPv6 address in the "IP address" field.

Q. Where can I find the IPv6 address ranges for Amazon Route 53's DNS servers and health checkers?

AWS now publishes its current IP address ranges in JSON format. To view the current ranges, download the .json file using the following link. If you access this file programmatically, ensure that the application downloads the file only after successfully verifying the TLS certificate that is returned by the AWS server.

Download: [ip-ranges.json](https://ip-ranges.amazonaws.com/ip-ranges.json) (<https://ip-ranges.amazonaws.com/ip-ranges.json>)

To find IP ranges for Route 53 servers, search for the following values in the "service" field:

Route 53 DNS servers: Search for "ROUTE53"

Route 53 health checkers: Search for "ROUTE53_HEALTHCHECKS"

For more information, see AWS IP Address Ranges (<http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>) in the Amazon Web Services General Reference.

Please note that the IPv6 ranges may not yet appear in this file. For reference, the IPv6 ranges for Amazon Route 53 health checkers are as follows:

2600:1f1c:7ff:f800::/53
2a05:d018:fff:f800::/53
2600:1f1e:7ff:f800::/53
2600:1f1c:fff:f800::/53
2600:1f18:3ff:f800::/53
2600:1f14:7ff:f800::/53
2600:1f14:fff:f800::/53
2406:da14:7ff:f800::/53
2406:da14:fff:f800::/53
2406:da18:7ff:f800::/53
2406:da1c:7ff:f800::/53
2406:da1c:fff:f800::/53
2406:da18:fff:f800::/53
2600:1f18:7ff:f800::/53
2a05:d018:7ff:f800::/53
2600:1f1e:fff:f800::/53
2620:107:300f::36b7:ff80/122
2a01:578:3::36e4:1000/122
2804:800:ff00::36e8:2840/122
2620:107:300f::36f1:2040/122
2406:da00:ff00::36f3:1fc0/122
2620:108:700f::36f4:34c0/122
2620:108:700f::36f5:a800/122
2400:6700:ff00::36f8:dc00/122
2400:6700:ff00::36fa:fdc0/122
2400:6500:ff00::36fb:1f80/122
2403:b300:ff00::36fc:4f80/122
2403:b300:ff00::36fc:fec0/122
2400:6500:ff00::36ff:fec0/122
2406:da00:ff00::6b17:ff00/122
2a01:578:3::b022:9fc0/122
2804:800:ff00::b147:cf80/122

Domain Name Registration

Q. Can I register domain names with Amazon Route 53?

Yes. You can use the AWS Management Console or API to register new domain names with Route 53. You can also request to transfer in existing domain names from other registrars to be managed by Route 53. Domain name registration services are provided under our Domain Name Registration Agreement (<https://aws.amazon.com/route53/domain-registration-agreement/>).

Q. What Top Level Domains (“TLDs”) do you offer?

Route 53 offers a wide selection of both generic Top Level Domains (“gTLDs”: for example, .com and .net) and country-code Top Level Domains (“ccTLDs”: for example, .de and .fr). For the complete list, please see the Route 53 Domain Registration Price List (https://d32ze2gidvkk54.cloudfront.net/Amazon_Route_53_Domain_Registration_Pricing_20140731.pdf).

Q. How can I register a domain name with Route 53?

To get started, log into your account and click on “Domains”. Then, click the big blue “Register Domain” button and complete the registration process.

Q. How long does it take to register a domain name?

Depending on the TLD you’ve selected, registration can take from a few minutes to several hours. Once the domain is successfully registered, it will show up in your account.

Q. How long is my domain name registered for?

The initial registration period is typically one year, although the registries for some top-level domains (TLDs) have longer registration periods. When you register a domain with Amazon Route 53 or you transfer domain registration to Amazon Route 53, we configure the domain to renew automatically. For more information, see [Renewing Registration](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-renew.html) (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-renew.html>) for a Domain in the Amazon Route 53 Developer Guide.

Q. What information do I need to provide to register a domain name?

In order to register a domain name, you need to provide contact information for the registrant of the domain, including name, address, phone number, and email address. If the administrative and technical contacts are different, you need to provide that contact information, too.

Q. Why do I need to provide personal information to register a domain?

ICANN, the governing body for domain registration, requires that registrars provide contact information, including

name, address, and phone number, for every domain name registration, and that registrars make this information publicly available via a Whois database. For domain names that you register as an individual (i.e., not as a company or organization), Route 53 provides privacy protection, which hides your personal phone number, email address, and physical address, free of charge. Instead, the Whois contains the registrar's name and mailing address, along with a registrar-generated forwarding email address that third parties may use if they wish to contact you.

Q. Does Route 53 offer privacy protection for domain names I have registered?

Yes, Route 53 provides privacy protection at no additional charge. The privacy protection hides your phone number, email address, and physical address. Your first and last name will be hidden if the TLD registry and registrar allow it. When you enable privacy protection, a Whois query for the domain will contain the registrar's mailing address in place of your physical address, and the registrar's name in place of your name (if allowed). Your email address will be a registrar-generated forwarding email address that third parties may use if they wish to contact you. Domain names registered by companies or organizations are eligible for privacy protection if the TLD registry and registrar allow it.

Q. Where can I find the requirements for specific TLDs?

For a list of TLDs please see the price list (https://d332ze2gidvkk54.cloudfront.net/Amazon_Route_53_Domain_Registration_Pricing_20140731.pdf) and for the specific registration requirements for each, please see the Amazon Route 53 Developer Guide (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/registrar-tld-list.html>) and our Domain Name Registration Agreement (<https://aws.amazon.com/route53/domain-registration-agreement/>).

Q. What name servers are used to register my domain name?

When your domain name is created we automatically associate your domain with four unique Route 53 name servers, known as a delegation set. You can view the delegation set for your domain in the Amazon Route 53 console. They're listed in the hosted zone that we create for you automatically when you register a domain.

By default, Route 53 will assign a new, unique delegation set for each hosted zone you create. However, you can also use the Route 53 API to create a "reusable delegation set", which you can then apply to multiple hosted zones that you create. For customers with large numbers of domain names, reusable delegation sets make migration to Route 53 simple, because you can instruct your domain name registrar to use the same delegation set for all your domains managed by Route 53. This feature also makes it possible for you to create "white label" name server addresses such as ns1.example.com, ns2.example.com, etc., which you can point to your Route 53 name servers. You can then use your "white label" name server addresses as the authoritative name servers for as many of your domain names as desired. For more details, see the Amazon Route 53 documentation (<http://docs.aws.amazon.com/Route53/latest/APIReference/actions-on-reusable-delegation-sets.html>).

Q. Will I be charged for my name servers?

You will be charged for the hosted zone that Route 53 creates for your domain name, as well as for the DNS queries against this hosted zone that Route 53 serves on your behalf. If you do not wish to be charged for Route 53's DNS service, you can delete your Route 53 hosted zone. Please note that some TLDs require you to have valid name servers as part of your domain name registration. For a domain name under one of these TLDs, you will need to procure DNS service from another provider and enter that provider's name server addresses before you can safely delete your Route 53 hosted zone for that domain name.

Q. What is Amazon Registrar, Inc. and what is a registrar of record?

AWS resells domain names that are registered with ICANN-accredited registrars. Amazon Registrar, Inc. is an Amazon company that is accredited by ICANN to register domains. The registrar of record is the "Sponsoring Registrar" listed in the WHOIS record for your domain to indicate which registrar your domain is registered with.

Q. Who is Gandi?

Amazon is a reseller of the registrar Gandi. As the registrar of record, Gandi is required by ICANN to contact the registrant to verify their contact information at the time of initial registration. You MUST verify your contact information if requested by Gandi within the first 15 days of registration in order to prevent your domain name from being suspended. Gandi also sends out reminder notices before the domain comes up for renewal.

Q. Which top-level domains does Amazon Route 53 register through Amazon Registrar and which ones does it register through Gandi?

See our documentation (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/registrar-tld-list.html>) for a list of the domains that you can currently register using Amazon Route 53. This list includes information about which registrar is the current registrar of record for each TLD that we sell.

Q. Can I transfer my .com and .net domain registrations from Gandi to Amazon?

No. We plan to add this functionality soon.

Q. What is Whois? Why is my information shown in Whois?

Whois is a publicly available database for domain names that lists the contact information and the name servers that are associated with a domain name. Anyone can access the Whois database by using the WHOIS command, which is widely available. It's included in many operating systems, and it's also available as a web application on many websites. The Internet Corporation for Assigned Names and Numbers (ICANN) requires that all domain names have publicly available contact information in case someone needs to get in contact with the domain name holder.

Q. How do I transfer my domain name to Route 53?

To get started, log into your account and click on "Domains". Then, click the "Transfer Domain" button at the top of the screen and complete the transfer process. Please make sure before you start the transfer process, (1) your

domain name is unlocked at your current registrar, (2) you have disabled privacy protection on your domain name (if applicable), and (3) that you have obtained the valid Authorization Code, or “authcode”, from your current registrar which you will need to enter as part of the transfer process.

Q. How do I transfer my existing domain name registration to Amazon Route 53 without disrupting my existing web traffic?

First, you need to get a list of the DNS record data for your domain name, generally available in the form of a “zone file” that you can get from your existing DNS provider. With the DNS record data in hand, you can use Route 53’s Management Console or simple web-services interface to create a hosted zone that can store the DNS records for your domain name and follow its transfer process, which will include such steps as updating the name servers for your domain name to the ones associated with your hosted zone. To complete the domain name transfer process, contact the registrar with whom you registered your domain name and follow its transfer process, which will include steps such as updating the name servers for your domain name to the ones associated with your hosted zone. As soon as your registrar propagates the new name server delegations, the DNS queries from your end users will start to get answered by the Route 53 DNS servers.

Q. How do I check on the status of my transfer request?

You can view the status of domain name transfers in the “Alerts” section on the homepage of the Route 53 console.

Q. What do I do if my transfer wasn’t successful?

You will need to contact your current registrar in order to determine why your transfer failed. Once they have resolved the issue, you can resubmit your transfer request.

Q. How do I transfer my domain name to a different registrar?

In order to move your domain name away from Route 53, you need to initiate a transfer request with your new registrar. They will request the domain name be moved to their management.

Q. Is there a limit to the number of domains I can manage using Amazon Route 53?

Each new Amazon Route 53 account is limited to a maximum of 50 domains. Complete our request form for a higher limit (<https://aws.amazon.com/route53-request/>) and we will respond to your request within two business days.

Q. Does Amazon Route 53 DNS support DNSSEC?

Amazon Route 53’s DNS services does NOT support DNSSEC at this time. However, our domain name registration service supports configuration of signed DNSSEC keys for domains when DNS service is configured at another provider. More information on configuring DNSSEC for your domain name registration can be found here (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html>).

Q. How do I transfer a domain registration that has DNSSEC enabled to Amazon Route 53?

See our documentation (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html>) for a step-by-step guide on transferring your DNSSEC-enabled domain to Amazon Route 53.

Route 53 Resolver

Q. What is Amazon Route 53 Resolver?

Route 53 Resolver is a regional DNS service that provides recursive DNS lookups for names hosted in EC2 as well as public names on the internet. This functionality is available by default in every Amazon Virtual Private Cloud (VPC). For hybrid cloud scenarios you can configure conditional forwarding rules and DNS endpoints to enable DNS resolution across AWS Direct Connect and AWS Managed VPN.

Q. What is recursive DNS?

Amazon Route 53 is both an Authoritative DNS service and Recursive DNS service. Authoritative DNS contains the final answer to a DNS query, generally an IP address. Clients (such as mobile devices, applications running in the cloud, or servers in your datacenter) don't actually talk directly to authoritative DNS services, except in very rare cases. Instead, clients talk to recursive DNS services (also known as DNS resolvers) which find the correct authoritative answer for any DNS query. Route 53 Resolver is a recursive DNS service.

When receiving a query, a recursive DNS service like Route 53 Resolver may either be configured to automatically forward the query directly to a specific recursive DNS server, or it may recursively search beginning with the root of the domain and continuing until it finds the final answer. In either case, once an answer is found, the recursive DNS server may cache the answer for a period of time so it can answer subsequent queries for the same name more quickly in the future.

Q. What are conditional forwarding rules?

Conditional forwarding rules allow Resolver to forward queries for specified domains to the target IP address of your choice, typically an on-premises DNS resolver. Rules are applied at the VPC level and can be managed from one account and shared across multiple accounts.

Q. What are DNS endpoints?

A DNS endpoint includes one or more elastic network interfaces (ENI) that attach to your Amazon Virtual Private Cloud (VPC). Each ENI is assigned an IP address from the subnet space of the VPC where it is located. This IP address can then serve as a forwarding target for on-premises DNS servers to forward queries. Endpoints are required both for DNS query traffic that you're forwarding from VPCs to your network and from your network to your VPCs over AWS Direct Connect and Managed VPN.

Q. How do I share rules across accounts?

Route 53 Resolver is integrated with AWS Resource Access Manager (RAM) which provides customers with a simple way to share their resources across AWS accounts or within their AWS Organization. Rules can be created in one primary account and then shared across multiple accounts using RAM. Once shared, the rules still need to be applied to VPCs in those accounts before they can take effect. For more information, see the AWS RAM documentation (https://docs.aws.amazon.com/ram/index.html#lang/en_us).

Q. What happens if I decide to stop sharing rules with other accounts?

Those rules will no longer be usable by the accounts you previously shared them with. This means that if those rules were associated to VPCs in those accounts, they will be disassociated from those VPCs.

Q. What regions are available for Route 53 Resolver?

Visit our AWS Region Table (<https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/>) to see which regions Route 53 Resolver has launched in.

Q. Does regional support for Route 53 Resolver mean that all of Amazon Route 53 is now regional?

No. Amazon Route 53 public and private DNS, traffic flow, health checks, and domain name registration are all global services.

Q. How do I get started with Route 53 Resolver?

Visit the Amazon Route 53 developer guide (<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html>) for details on getting started. You can also configure Resolver from within the Amazon Route 53 console.



Learn more about Amazon Route 53 pricing

Simple pricing to only pay for what you need.

Learn more



Sign up for a free account

Instantly get access to the AWS Free Tier.

Sign up (https://portal.aws.amazon.com/gp/aws/developer/registration/index.html?nc2=h_ct&src=header_signup)



Start building in the console

Get started with Amazon Route 53 in the AWS Console.

Sign in (<https://console.aws.amazon.com/route53/home>)

Register for re:Invent Bootcamps

Learn from AWS experts at exam prep bootcamps - space is limited!



(https://reinvent.awsevents.com/learn/bootcamps/?sc_icampaign=aware_reinvent_bootcamps2019_aws&sc_ichannel=ha&sc_icontent=awssm-2448&sc_iplace=2up&trk=ha_awssm-2448)

Get AWS Certified

AWS Certifications can help you advance your career and boost your earning power



(https://pages.awscloud.com/tc_get-aws-certified.html?sc_icampaign=aware_getcertified_evergreen2019&sc_ichannel=ha&sc_icontent=awssm-2655&sc_iplace=2up&trk=ha_awssm-2655)

AWS re:Invent | December 2 – 6, 2019 | Las Vegas, Nevada

Invite your friends to register for re:Invent, and compete to win a VIP experience on-site plus free passes to Intersect. [Learn more >>](#)

AWS re:Invent

(https://reinvent.awsevents.com/vip/?sc_icampaign=Event_reInvent_2019_1up_DG3_VIP&sc_ichannel=ha&sc_icontent=awssm-2785&sc_ioutcome=Strategic_Events&sc_iplace=1up&trk=ha_a131L0000057yyxQAA~ha_awssm-2785&trkCampaign=AWS_reInvent_2019)

Page Content

Getting Started Domain Name System (DNS) DNS Routing Policies Traffic Flow Private DNS Health Checks & DNS

Failover Domain Name Registration Route 53 Resolver

[aws.amazon.com \(https://aws.amazon.com/route53/faqs/\)](https://aws.amazon.com/route53/faqs/)